Critical Foundations

Protecting America's Infrastructures

The Report of the President's Commission
on Critical Infrastructure Protection

October 1997

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

DTIC QUALITY INSPECTED 2

19971114 064

PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION

October 13, 1997

The President
The White House
Washington, DC 20500

Dear Mr. President:

It is a privilege to forward the report of the President's Commission on Critical Infrastructure Protection, *Critical Foundations*. You asked us to study the critical infrastructures that constitute the life support systems of our nation, determine their vulnerabilities and propose a strategy for protecting them into the future. I believe our report does this.

There is no doubt that our critical infrastructures are the best in the world—largely the result of the tremendous efficiency and global reach made possible by incorporation of our rapidly advancing information and communication technology. In fact, we found all our infrastructures increasingly dependent on information and communications systems that criss-cross the nation and span the globe. That dependence is the source of rising vulnerabilities and, therefore, it is where we concentrated our effort.

We found no evidence of an impending cyber attack which could have a debilitating effect on the nation's critical infrastructures. While we see no electronic disaster around the corner, this is no basis for complacency. We did find widespread capability to exploit infrastructure vulnerabilities. The capability to do harm—particularly through information networks—is real; it is growing at an alarming rate; and we have little defense against it.

Because the infrastructures are mainly privately owned and operated, we concluded that critical infrastructure assurance is a shared responsibility of the public and private sectors. The only sure path to protected infrastructures in the years ahead is through a real partnership between infrastructure owners and operators and the government. Consequently, in addition to our recommendations about improving our government's focus on infrastructure assurance in the Information Age, you will find some recommendations for collaborative public and private organizational arrangements that challenge our conventional way of thinking about government and private sector interaction.

Thank you for the opportunity to serve our nation on this Commission, and for the chance to work with a talented and patriotic group of Commissioners and staff from both government and the private sector.

Respectfully,

Robert T. Marsh
Chairman

P.O. BOX 46258, WASHINGTON, DC 20050-6258

(Intentionally Left Blank)

President's Commission on Critical Infrastructure Protection

COMMISSIONERS

Robert T. Marsh, *Chairman*

John R. Powers, *Executive Director — Federal Emergency Management Agency*
Merritt E. Adams — *AT&T*
Richard P. Case — *IBM*
Mary J. Culnan — *Georgetown University*
Peter H. Daly — *Department of the Treasury*
John C. Davis — *National Security Agency*
Thomas J. Falvey — *Department of Transportation*
Brenton C. Greene — *Department of Defense*
William J. Harris — *Association of American Railroads*
David A. Jones — *Department of Energy*
William B. Joyce — *Central Intelligence Agency*
David V. Keyes — *Federal Bureau of Investigation*
Stevan D. Mitchell — *Department of Justice*
Joseph J. Moorcones — *National Security Agency*
Irwin M. Pikus — *Department of Commerce*
William Paul Rodgers, Jr. — *National Association of Regulatory Utility Commissioners*
Susan V. Simens — *Federal Bureau of Investigation*
Frederick M. Struble — *Federal Reserve Board*
Nancy J. Wong — *Pacific Gas and Electric Company*

EXECUTIVE STAFF

Phillip E. Lacombe, *Staff Director*
James H. Kurtz, COL, USA, *Chief of Staff/Executive Secretary*

Janet B. Abrams, *Director of External Affairs/White House Liaison*
Robert E. Giovagnoni, Col, USAF, *General Counsel*
Adrienne M. Griffen, *Executive Assistant to the Chairman*
Elizabeth (Betsy) Harrison, *Director of Legislative Affairs*
Brian P. Hoey, Lt Col, USAF, *Executive Assistant to the Chairman*
Nelson M. McCouch III, MAJ, USA, *Director of Public Affairs*
Monica Y. McNeil, *Executive Assistant to the Chief of Staff/Assistant Executive Secretary*
Annie N. Nelson, *Director of Administration*
Carla L. Sims, *Director of Public Affairs*
Lawrence P. St. Marie, SMSgt, USAF, *Executive Officer*
Sona A. Virdi, *Executive Assistant to the Staff Director*

PROFESSIONAL STAFF

Elizabeth A. Banker
Gary R. Boyd
Patricia E. Burt
Julie Consilvio
Frederick S. Davidson
L. C. J. Jacobson
Gary P. Kosciusko
Lloyd E. Lutz Jr., Lt Col, USAF
Carol M. Medill
T. Lynette Proctor
Pamela D. Saunders
James J. Stekert
Stephen T. York

SUPPORT STAFF

Bernard R. Robinson, *Deputy Director of Administration*
Bonnie L. Julia, SFC, USA, *NCOIC*

Karen R. Allen, SrA, USAF
Robert W. Boyd, YN2, USN
Joseph A. Broadway, YN1, USN
Patrick Barlow
Eric J. Cline
James E. Crawford, SSG, USA
Debra A. Dawson, SSG, USA
Roada Dickerson, SrA, USAF
Elizabeth S. Ellingboe, SSgt, USAF
Jeffrey G. Estep, SSgt, USAF
Troy L. Joyner, SSG, USA
Peter D. LeNard
Becky Love
Gerald T. Posey, TSgt, USAF
Sandra M. Robinson, SSgt, USAF
Sandra L. Scroggs
Mike Seabron
Sherrie M. Smith, SGT, USA
Sharon S. Strippoli
Shawn R.L. Vincent, Sgt, USAF
Scott A. Ward
Brian W. Young, SrA, USAF
Ed Young

SENIOR CONSULTANTS

William A. Buehring
Mary F. Dunham
Ron E. Fisher
Paul W. Hanley
Peter Gossens
Duane G. Harder
Michael T. Hovey
Joelle Jordan
Ramesh Maraj
Gabe Maznick
Willis J. Ozier
Paul Byron Pattak
James P. Peerenboom
George J. Rothstein
Lee M. Zeichner

And special thanks to the following for their advice and support:

Ed Appel
Frederick L. Frostic
Bill Garber
Seymour Goodman
David Graham
Michael Leonard
Stephen J. Lukasik
Paul H. Richanbach
Kathleen Robertson
Elizabeth Sauer
Paula Scalingi
James Schlesinger
Suzy Tichenor
Larry Welch

Contents

		Page
Foreword		vii
Executive Summary		ix
Part One: The Case for Action		1
Chapter One	Acting Now to Protect the Future	3
Chapter Two	The New Geography	7
Chapter Three	New Vulnerabilities, Shared Threats, Shared Responsibility	11
Chapter Four	Findings and Policy	21
Part Two: A Strategy for Action		25
Chapter Five	Establishing the Partnership	27
Chapter Six	Building the Partnership	35
Chapter Seven	Structuring the Partnership	47
Chapter Eight	Report on Awareness and Education	67
Chapter Nine	Leading by Example	73
Chapter Ten	Legal Initiatives	79
Chapter Eleven	Research and Development	89
Chapter Twelve	Implementation Strategy	93
Onward		101
Appendices		
Appendix A	Sector Summary Reports	A-1
Appendix B	Glossary	B-1

(Intentionally Left Blank)

Foreword

The task given us by the President was daunting. America's critical infrastructures underpin every aspect of our lives. They are the foundations of our prosperity, enablers of our defense, and the vanguard of our future. They empower every element of our society. There is no more urgent priority than assuring the security, continuity, and availability of our critical infrastructures.

After fifteen months of evaluating the infrastructures, assessing their vulnerabilities, and deliberating assurance alternatives, our fundamental conclusion is that we have to think differently about infrastructure protection today and for the future.

We found that the nation is so dependent on our infrastructures that we must view them through a national security lens. They are essential to the nation's security, economic health, and social well being. In short, they are the lifelines on which we as a nation depend.

We also found the collective dependence on the information and communications infrastructure drives us to seek new understanding about the Information Age. Essentially, we recognize a very real and growing cyber dimension associated with infrastructure assurance.

In the cyber dimension there are no boundaries. Our infrastructures are exposed to new vulnerabilities—cyber vulnerabilities—and new threats—cyber threats. And perhaps most difficult of all, the defenses that served us so well in the past offer little protection from the cyber threat. Our infrastructures can now be struck directly by a variety of malicious tools.

Our new thinking must accommodate the cyber dimension. We must develop a new set of "street smarts" to deal with it, and we must apply them in new ways. One of the most important is recognizing that the owners and operators of our critical infrastructures are now on the front lines of our security effort. They are the ones most vulnerable to cyber attacks. And that vulnerability jeopardizes our national security, global economic competitiveness, and domestic well being.

It is with this in mind that we offer our report.

(Intentionally Left Blank)

Executive Summary

Critical Foundations
Protecting America's Infrastructures

"Our responsibility is to build the world of tomorrow by embarking on a period of construction—one based on current realities but enduring American values and interests ...."

— President William J. Clinton, "A National Security Strategy for a New Century," May 1997

Introduction

Our national defense, economic prosperity, and quality of life have long depended on the essential services that underpin our society. These critical infrastructures—energy, banking and finance, transportation, vital human services, and telecommunications—must be viewed in a new context in the Information Age. The rapid proliferation and integration of telecommunications and computer systems have connected infrastructures to one another in a complex network of interdependence. This interlinkage has created a new dimension of vulnerability, which, when combined with an emerging constellation of threats, poses unprecedented national risk.

For most of our history, broad oceans, peaceable neighbors and our military power provided all the infrastructure protection we needed. But just as the terrible long-range weapons of the Nuclear Age made us think differently about security in the last half of the 20th Century, the electronic technology of the Information Age challenges us to invent new ways of protecting ourselves now. We must learn to negotiate a new geography, where borders are irrelevant and distances meaningless, where an enemy may be able to harm the vital systems we depend on without confronting our military power. National defense is no longer the exclusive preserve of government, and economic security is no longer just about business. The critical infrastructures are central to our national defense and our economic power, and we must lay the foundations for their future security on a new form of cooperation between government and the private sector.

The Case for Action

A satchel of dynamite and a truckload of fertilizer and diesel fuel are known terrorist tools. Today, the right command sent over a network to a power generating station's control computer could be just as devastating as a backpack full of explosives, and the perpetrator would be more difficult to identify and apprehend.

The rapid growth of a computer-literate population ensures that increasing millions of people around the world possess the skills necessary to conduct such an attack. The wide adoption of common protocols for system interconnection and the availability of "hacker tool" libraries make their task easier.

While the possibility of chemical, biological, and even nuclear weapons falling into the hands of terrorists adds a new and frightening dimension to physical attacks, such weapons are difficult to acquire. In contrast, the resources necessary to conduct a cyber attack have shifted in the past few years from the arcane to the commonplace. A personal computer and a telephone connection to an Internet Service Provider anywhere in the world are enough to cause harm.

Growing complexity and interdependence, especially in the energy and communications infrastructures, create an increased possibility that a rather minor and routine disturbance can cascade into a regional outage. Technical complexity may also permit interdependencies and vulnerabilities to go unrecognized until a major failure occurs.

We know our infrastructures have substantial vulnerabilities to domestic and international threats. Some have been exploited—so far chiefly by insiders. Although we know these new vulnerabilities place our infrastructures at risk, we also recognize that this is a new kind of risk that requires new thinking to develop effective countermeasures. Coping with increasingly cyber-based threats demands a new approach to the relationship between government and the private sector. Because it may be impossible to determine the nature of a threat until after it has materialized, infrastructure owners and operators—most of whom are in the private sector—must focus on protecting themselves against the tools of disruption, while the government helps by collecting and disseminating the latest information about those tools and their employment. This cooperation implies a more intimate level of mutual communication, accommodation, and support than has characterized public-private sector relations in the past.

The Commission has not discovered an immediate threat sufficient to warrant a fear of imminent national crisis. However, we are convinced that our vulnerabilities are increasing steadily, that the means to exploit those weaknesses are readily available and that the costs associated with an effective attack continue to drop. What is more, the investments required to improve the situation—now still relatively modest—will rise if we procrastinate.

We should attend to our critical foundations before we are confronted with a crisis, not after. Waiting for disaster would prove as expensive as it would be irresponsible.

A Strategy for Action

The Commission recommends several practical measures to realize our vision of a new government-private sector partnership.

The quickest and most effective way to achieve a much higher level of protection from cyber threats is a strategy of cooperation and information sharing based on partnerships among the infrastructure owners and operators and appropriate government agencies.

To facilitate this new relationship between government and industry, new mechanisms will be needed, including sector "clearing houses" to provide the focus for industry cooperation and information sharing; a council of industry CEOs, representatives of state and local government, and Cabinet secretaries to provide policy advice and implementation commitment; a real-time capability for attack warning; and a top-level policy making office in the White House.

Other measures are also required. Infrastructure protection must be ingrained in our culture, beginning with a comprehensive program of education and awareness. This includes both infrastructure stakeholders and the general public, and must extend through all levels of education, both academic and professional.

The federal government must lead the way into the Information Age by example, tightening measures to protect the infrastructures it operates against physical and cyber attack.

The government can also help by streamlining and clarifying elements of the legal structure that have not kept pace with technology. Some laws capable of promoting assurance are not as clear or effective as they could be. Others can operate in ways that may be unfriendly to security concerns. Sorting them out will be an extensive undertaking, involving efforts at local, state, federal, and international levels. We have offered a number of preliminary legal recommendations intended to jump-start this process of reform.

Another area where government must lead is in research and development. Some of the basic technology and tools needed to provide improved infrastructure protection already exist, but need to be widely employed. However, there is a need for additional technology with which to protect our essential systems. We have, therefore, recommended a program of research and development focused on those needed capabilities.

In summary, all of us need to recognize that the cyber revolution brings us into a new age as surely as the industrial revolution did two centuries ago. Now, as then, our continued security requires a reordering of national priorities and new understanding about our respective roles in support of the national goals. The relationships that have stood us in such good stead through the end of the second millennium must give way to new ones better suited to the third.

(Intentionally Left Blank)

Part One

The Case for Action

(Intentionally Left Blank)

Chapter One

Acting Now to Protect the Future

"We are at the dawn of a new century. Now is the moment to be farsighted as we chart a path into the new millennium."

— President William J. Clinton, "A National Security Strategy for a New Century," May 1997

Life is good in America because things work. When we flip the switch, the lights come on. When we turn the tap, clean water flows. When we pick up the phone, our call goes through. We are able to assume that things will work because our *infrastructures* are highly developed and highly effective. By *infrastructure* we mean more than just a collection of individual companies engaged in related activities; we mean a network of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services.

Businesses, too, depend on infrastructures. Private companies are able to guarantee on-time performance because our infrastructures permit low cost transport and instantaneous tracking of shipments. Managers take for granted that the goods and services essential to their operations will be there when needed.

Reliable and secure infrastructures are thus the foundation for creating the wealth of our nation and our quality of life as a people. They are fundamental to development and projection of the military power that enables our diplomacy to be effective. They make it possible for us to enjoy our inalienable rights and take advantage of the freedoms on which our nation was founded. Certain of our infrastructures are so vital that their incapacity or destruction would have a debilitating impact on our defense and economic security.

The ***transportation*** infrastructure moves goods and people within and beyond our borders, and makes it possible for the United States to play a leading role in the global economy.

The ***oil and gas production and storage*** infrastructure fuels transportation services, manufacturing operations, and home utilities.

The ***water supply*** infrastructure assures a steady flow of water for agriculture, industry (including various manufacturing processes, power generation, and cooling), business, firefighting, and our homes.

The ***emergency services*** infrastructure in communities across the country responds to our urgent police, fire, and medical needs, saving lives and preserving property.

The ***government services*** infrastructure consists of federal, state, and local agencies that provide essential services to the public, promoting the general welfare.

The ***banking and finance*** infrastructure manages trillions of dollars, from deposit of our individual paychecks to the transfer of huge amounts in support of major global enterprises.

The ***electrical power*** infrastructure consists of generation, transmission, and distribution systems that are essential to all other infrastructures and every aspect of our economy. Without electricity, our factories would cease production, our televisions would fade to black, and our radios would fall silent (even a battery-powered receiver depends on an electric-powered transmitter). Our street intersections would suddenly be dangerous. Our homes and businesses would go dark. Our computers and our telecommunications would no longer operate.

The ***telecommunications*** infrastructure has been revolutionized by advances in information technology in the past two decades to form an ***information and communications*** infrastructure, consisting of the Public Telecommunications Network (PTN), the Internet, and the many millions of computers in home, commercial, academic, and government use. Taking advantage of the speed, efficiency and effectiveness of computers and digital communications, all the critical infrastructures are increasingly connected to networks, particularly the Internet. Thus, they are connected to one another. Networking enables the electronic transfer of funds, the distribution of electrical power, and the control of gas and oil pipeline systems. Networking is essential to a service economy as well as to competitive manufacturing and efficient delivery of raw materials and finished goods. The information and communications infrastructure is basic to responsive emergency services. It is the backbone of our military command and control system. And it is becoming the core of our educational system.

Disruption of any infrastructure is always inconvenient and can be costly and even life threatening. Major disruptions could lead to major losses and affect national security, the economy, and the public good. Mutual dependence and the interconnectedness made possible by the information and communications infrastructure lead to the possibility that our infrastructures may be vulnerable in ways they never have been before. Intentional exploitation of these new vulnerabilities could have severe consequences for our economy, security, and way of life.

Technologies and techniques that have fueled major improvements in the performance of our infrastructures can also be used to disrupt them. The United States, where close to half of all computer capacity and 60 percent of Internet assets reside, is at once the world's most advanced and most dependent user of information technology. More than any other country, we rely on a set of increasingly accessible and technologically reliable infrastructures, which in turn have a

growing collective dependence on domestic and global networks. This provides great opportunity, but it also presents new vulnerabilities that can be exploited. It heightens risk of cascading technological failure, and therefore of cascading disruption in the flow of essential goods and services. Computerized interaction within and among infrastructures has become so complex that it may be possible to do harm in ways we cannot yet conceive.

The threat is real enough. The terrorist bombings of the US World Trade Center, the federal building in Oklahoma City, and the El Khobar quarters in Saudi Arabia have demonstrated all too well the malevolent intent of some parties toward the United States. Skilled computer operators have demonstrated their ability to gain access to networks without authorization. Some do it for the thrill or the notoriety. Some do it for financial gain. Some do it to further a cause. Whatever the motivation, their success in entering networks to alter data, extract financial or proprietary information, or introduce viruses demonstrates that it can be done and gives rise to concerns that, in the future, some party wishing to do serious damage to the United States will do so by the same means.

Real vulnerabilities also exist. Infrastructures have always been subject to local or regional outages resulting from earthquakes, storms, and floods. Their owners and operators, in cooperation with local, state, and federal emergency services, have demonstrated their capacity to restore services efficiently. Physical vulnerabilities to man-made threats, such as arson and bombs, are likewise not new. But physical vulnerabilities take on added significance as new capabilities to exploit them emerge, including chemical, biological, and even nuclear weapons. As weapons of mass destruction proliferate, the likelihood of their use by terrorists increases.

Terrorist attacks have typically been against single targets—individuals, buildings, or institutions. Today, more sophisticated physical attacks may also exploit the emerging vulnerabilities associated with the complexity and interconnectedness of our infrastructures. Bombs—even homemade ones—have always been able to damage a pipeline, electrical power transformer, telecommunications switching station, or microwave relay antenna. In the networked world of today, the effects of such physical attacks could spread far beyond the radius of a bomb blast. Adding to our physical vulnerability is the fact that information readily available on the World Wide Web (WWW) may disclose to a terrorist the best place to set explosive charges for maximum disruptive effects.

Our dependence on the information and communications infrastructure has created new cyber vulnerabilities, which we are only starting to understand. In addition to the disruption of information and communications, we also face the possibility that someone will be able to actually mount an attack against other infrastructures by exploiting their dependence on computers and telecommunications (see Figure 1).

Physical means to exploit physical vulnerabilities probably remain the most worrisome threat to our infrastructures *today.* But almost every group we met voiced concerns about the new cyber vulnerabilities and threats. They emphasized the importance of developing approaches to protecting our infrastructures against cyber threats ***before*** they materialize and produce major system damage.

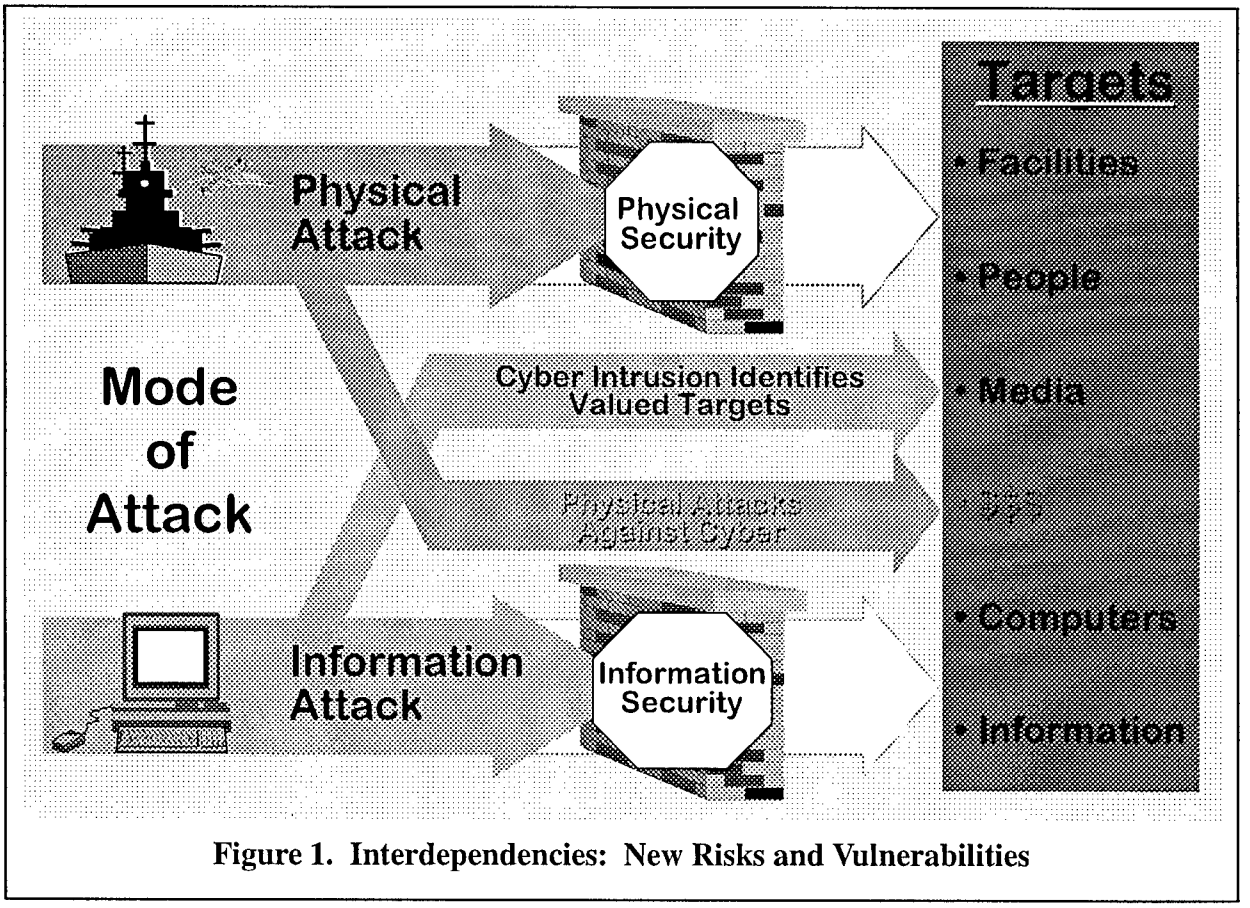


Figure 1. Interdependencies: New Risks and Vulnerabilities

We know our infrastructures have substantial vulnerabilities to domestic and international threats. Some have been exploited—so far chiefly by insiders. Protecting our infrastructures into the 21st Century requires that we develop greater understanding of their vulnerabilities and act decisively to reduce them. It was for just this purpose that President Clinton called into being the President's Commission on Critical Infrastructure Protection in July 1996. In the fifteen months since its creation, the Commission—drawn from the federal government and the private sector—has thoroughly reviewed the vulnerabilities and threats facing our infrastructures, assessed the risks, consulted with thousands of experts, and deliberated at length as to how best to assure our nation's critical foundations in the decades to come. Our analyses, findings, conclusions, and recommendations form the substance of this report.

Our fundamental conclusion is this:

Waiting for disaster is a dangerous strategy. Now is the time to act to protect our future.

Chapter Two

The New Geography

"As borders open and the flow of information, technology, money, trade, and people across borders increases, the line between domestic and foreign policy continues to blur."

— President William J. Clinton, "A National Security Strategy for a New Century," May 1997

Few enemies of the United States have ever had the means to seriously threaten our heartland. Even in the darkest early days of World War II, just after Pearl Harbor, no enemy had the shipping, landing craft, or forces to invade the continental US, or aircraft with the range to reach the mainland and return. For most of our history we've never had to worry much about being attacked at home; broad oceans east and west and peaceable neighbors north and south gave us all the protection we needed.

In the early 1950s, the geography that kept us safe was overcome by Soviet long-range bombers and intercontinental ballistic missiles aimed not only at our military capabilities, but also at the industries and institutions that give our nation its character. We had to learn to think differently about our safety and security. We built backyard bomb shelters, and whole generations of us practiced diving beneath our school desks at the sound of a siren. Our fear of surprise nuclear attack slowly faded as we developed satellites and other early warning capabilities that enabled us to overcome geography and detect a Soviet missile launch in time to launch our own missiles—thus ensuring the credibility of the deterrent policy of Mutual Assured Destruction.

The demise of the Soviet Union, "detargeting" of nuclear missiles, and strategic arms reductions appear to have left America once more relatively invulnerable to physical attack by foreign nations. However, as the threat of a nuclear war has diminished, new technologies have appeared that render physical geography less relevant and our domestic sanctuary less secure. Today, a computer can cause switches or valves to open and close, move funds from one account to another, or convey a military order almost as quickly over thousands of miles as it can from next door, and just as easily from a terrorist hideout as from an office cubicle or military command center. A computer message from Earth can steer a vehicle and point a camera on the surface of Mars. A false or malicious computer message can traverse multiple national borders, leaping from jurisdiction to jurisdiction to avoid identification, complicate lawful pursuit, or escape retribution.

Vulnerability to an adversary using cyber tools was examined during a military exercise[1] conducted in early summer of 1997. The scenario featured "scripted" attacks on the energy and telecommunications infrastructures (controllers injected incidents into the scenario; military commands and government agencies reacted as though the reported incidents were real). Companies providing electrical power in selected cities were subjected to scripted attack by cyber means, over time, in a way that made the resulting simulated outages appear to be random and unrelated. Concurrently, a "Red Team" used hacker techniques available on the Internet to attempt to penetrate Department of Defense (DoD) computers. With no insider information, and constrained by US law, the team spent three months probing the vulnerabilities of several hundred unclassified computer networks. They were able to penetrate many of these networks, and even gained system administrator level privileges in some.

Simulated cyber attacks on nearby privately owned energy companies and telecommunications service providers and successful penetrations into DoD computers were assessed by controllers as sufficient to have disrupted operations at selected military bases—creating a situation in which our ability to deploy and sustain military forces was degraded. Was this exercise an overstatement of today's vulnerabilities or a glimpse at future forms of terrorism and war? The experience to date, the known vulnerabilities, and the continuing pace of change suggest the latter.

In short, the day may be coming when an enemy can attack us from a distance, using cyber tools, without first confronting our military power and with a good chance of going undetected. The new geography is a borderless cyber geography whose major topographical features are technology and change.

But it is also a global geography. The world's economy is integrated as never before. With rapid movement of capital, labor, goods and services, technology, and above all, information, across frontiers, our businesses have global outlooks, customers, and needs. In this global economy, communications give even small nations equal access to markets. A nation may no longer need to control territory to have access to its resources.

These changes also have a dark side. As a result of global economic integration, made possible in large measure by information technology, operations of US infrastructures extend far beyond our national boundaries, and even beyond our control. As networks extend to new markets and new sources, new points of entry are established, providing conduits of attack to adversaries at home and abroad. International terrorism, narcotics trafficking, and transnational economic crime are also features—undesirable features—of the new geography.

[1] Chairman of the Joint Chiefs of Staff Exercise ELIGIBLE RECEIVER 1997.

Technology and Change

Fifteen years ago, there were few cell phones or computers and Internet access was limited. The World Wide Web did not exist, nor did today's widely used e-mail systems.

Today, in the United States alone, there are about 180 million computers. Worldwide, there are some 1.3 million local area networks. Computers communicate regionally, nationally, and globally across thousands of wide area networks or through the Internet.

The pace of technological change and our reliance on technology are suggested in Table 1, which compares worldwide populations of 1982 with those of a year ago and those projected to exist in 2002.[2] This table illustrates the growth in the number of potential targets for a cyber attack. It also shows the growth in the number of people having the technical skills necessary to launch such an attack. Of particular significance is the fact that in the past 15 years, the public telecommunications network has become increasingly software driven, remotely managed and maintained through computer networks. The last line of the table shows the population of systems control software specialists who possess the tools and know-how to disrupt or take down the public telecommunications network.

Table 1. Global Technology Trends

Category	15 Years Ago	1996	5 Years Hence
Personal Computers	Thousands	400 million	500 million
Local Area Networks	Thousands	1.3 million	2.5 million
Wide Area Networks	Hundreds	Thousands	Tens of thousands
Viruses	Some	Thousands	Tens of thousands
Internet Devices Accessing the World-Wide Web (WWW)	None	32 million	300 million
Population With Skills for a Cyber Attack	Thousands	17 million	19 million
Telecommunications Systems Control Software Specialists	Few	1.1 million	1.3 million

[2] Technical population data, programmers and telecommunications, 1982-2025, International Data Corporation, and e-mail and documents from the National Computer Security Center, National Security Agency, July 29, 1997.

Effects of the New Geography on Infrastructures

Profound change within the global marketplace, interdependency, restructuring, and reliance on technology make protection a continuing challenge for business and national leaders. The ever-expanding global information infrastructure underpins the global economy. Both business and government must adjust to a borderless world of unrestricted transactions and communications.

Many major infrastructure industries, particularly telecommunications and electricity, are being affected by deregulation and are restructuring to compete at home and in the global marketplace. Organizations have harnessed information technology to accelerate their delivery of goods and services, tighten the efficiency of their processes, and shed excess inventory and unused reserve capacity. Many businesses are so tightly balanced in their "just-in-time" processes that recovery from even a minor disruption would prove difficult.

In sum, technology and change produce better service at lower cost, new markets and more efficient processes throughout the nation and indeed the world. As a result, we depend more than ever on infrastructure services. But at the same time, market forces result in a diffusion of accountability, a decrease in "end-to-end" or system-wide analysis and responsibility, less research and development investment, and a reduction in reserve capacity. Today's processes are more efficient, but they lack the redundant characteristics that gave their predecessors more resilience.

All of us—government and business, service providers, and service consumers—must pay attention to, and think differently about, a new geography that is global in the physical dimension and without borders in the cyber dimension.

Chapter Three

New Vulnerabilities, Shared Threats, Shared Responsibility

"We face no imminent threat, but we do have an enemy—the enemy of our time is inaction."

— President William J. Clinton, State of the Union Address, January 1997

New Vulnerabilities

Each of the infrastructures is vulnerable in varying degrees to natural disasters, component failures, human negligence, and willful human misconduct. The Commission divided its work into five "sectors" based on the common characteristics of the included industries, and found a mix of physical vulnerabilities, many first identified in the 1980s, and newer cyber vulnerabilities. Results of the sector team studies are in Appendix A. Key points are summarized below.

Information and Communications

All critical infrastructures are increasingly dependent on information and communications. The most important impact and vulnerability for this sector is the increasing interdependency of the PTN and the Internet. The Internet depends heavily on the PTN. The PTN, in turn, depends on electrical power for operations and on telephone lines and fiber optic cables that often run along transportation routes. The PTN is increasingly software driven, and remotely managed and maintained through computer networks. Deregulation of the telecommunications industry will markedly increase the number of access points, increasing opportunities for attack.

One well-publicized example of vulnerability associated with our dependence on computers is the "Year 2000" problem, which, if not corrected, has the potential to adversely affect the operations of all our infrastructures. Solving the Year 2000 problem was not part of the Commission's mission, and efforts are under way elsewhere in the federal government and across the country to

remedy the problem before computer clocks turn to 00. But within the bounds of our mission, we did observe that resolving the Year 2000 problem requires the complete review and possibly the substantial revision of an affected organization's operational computer programs. Many people will have to be given access to these programs, as well as the authority to modify them and place them in service with less than adequate testing. The vulnerability will be worse if, as we expect, much of the review and modification work is contracted to outside, perhaps even foreign, firms. An adversary with access to a company's operational computer programs could understand aspects of the company's business practices better than the company's own management, which in turn would allow that adversary to design a subtle or comprehensive attack to gather information or reduce system effectiveness.

Energy

Prolonged disruption in the flow of energy would seriously affect every infrastructure.

The significant physical vulnerabilities for electric power are related to substations, generation facilities, and transmission lines. Large oil refineries are also attractive targets. The increase in transportation of oil via pipelines over the last decade provides a huge, attractive, and largely unprotected target array. Oil and gas vulnerabilities include lines at river crossings; interconnects; valves, pumps, and compressors; and natural gas city gates. Large metropolitan areas could be deprived of critical fuel for an extended period by a properly executed attack.

The widespread and increasing use of Supervisory Control and Data Acquisition (SCADA) systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means. The exponential growth of information system networks that interconnect the business, administrative, and operational systems contributes to system vulnerability.

Banking and Finance

The principal vulnerabilities of the banking and finance sector are physical in nature. Its payments systems and its securities and commodities exchanges with their clearing and settlement organizations are vital to other parts of the banking and financial system and the economy at large. There are few of them, and in some cases, they are geographically concentrated. To back up its payments systems, the Federal Reserve has three geographically dispersed and "hardened" sites, each capable of completing the full volume of transactions sent over its wire transfer system. Similar back-up and "hardening" of facilities can be found in the other electronic payments and messaging systems, and most exchanges have a variety of contingency arrangements to rechannel trading activities should anyone's facilities become inoperable. In addition, the principal clearing and settlement organizations for the major stock exchanges have back-up sites some distance from the primary sites, as well as cold storage sites for data. These arrangements, together with strong measures to "harden" primary facilities, greatly reduce the overall vulnerabilities of this sector, but there remains risk from any event that disrupts

telecommunications service and electric power within the geographic area in which key facilities are concentrated.

Physical Distribution

While the vulnerabilities of the physical distribution sector are still predominantly physical in nature, there are emerging cyber vulnerabilities as the sector increasingly relies on information technology to shorten lead times, route and schedule traffic and more—all on increasingly crowded communications channels. Physically most significant are the bridges over waterways, which are crossed by personal and commercial transportation, railroad tracks, telecommunications cables, and gas and oil pipelines. Vulnerabilities of the information and communications infrastructure also affect every aspect of the transportation industry. The most significant projected vulnerabilities are those associated with the modernization of the National Airspace System (NAS) and the plan to adopt the Global Positioning System (GPS) as the sole basis for radionavigation in the US by 2010.

Vital Human Services

Emergency responders are inadequately trained and equipped to respond to a chemical, biological, or nuclear attack on a civilian target. The 911 system can be overloaded through misuse and mischief, thereby missing life-and-death calls. Response coordination is vulnerable because the allocated radio frequencies used for responder communications are becoming congested and inadequate.

Treated water supplies do not have adequate physical protection to mitigate the threat of chemical or biological contamination, nor is there technology available to allow the detection, identification, measurement, and treatment of highly toxic, waterborne contaminants. Cyber vulnerabilities include the increasing reliance on SCADA systems for control of the flow and pressure of water supplies.

Government services are dependent on mega-databases of a highly confidential nature and containing information on private citizens. The uneven security practices of government agencies allow exploitation through the cyber vulnerabilities of these databases.

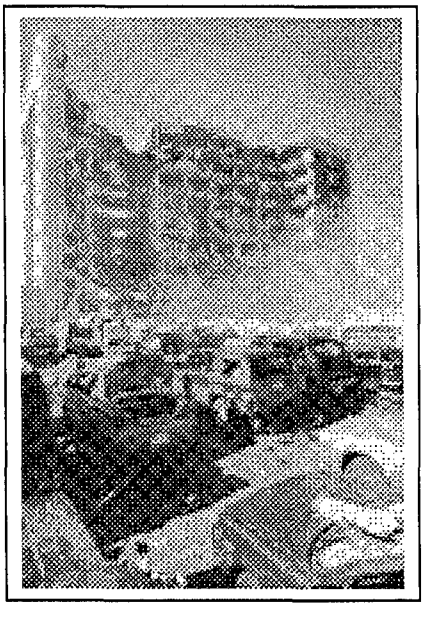
Shared Threats

A *threat* is traditionally defined as a *capability* linked to hostile *intent.* Linking capability to intent works well when malefactors are clearly discernible and US intelligence agencies can focus collection efforts to determine what capabilities they possess or are trying to acquire. During the Cold War, for example, weapons with potential to threaten the United States took years to develop, involved huge industrial complexes, and were on frequent display in large military exercises. Today, however, malefactors are no longer necessarily nation-states, and expensive weapons of war are joined by means that are easier to acquire, harder to detect, and have legitimate peacetime applications. The tools designed to access, manipulate, and manage the information or communications components that control critical infrastructures can also be used to do harm. They are inexpensive, readily available, and easy to use.

While poor design, accidents and natural disasters may threaten our infrastructures, we focused primarily on hostile attempts to damage, misuse, or otherwise subvert them. The Commission looked at both physical and cyber threats; however, we concentrated on the fundamentally new security challenges presented by networked information systems. Key points are summarized below.

Physical Threats

Physical threats fall into two general categories. The first includes threats posed by explosives, such as the World Trade Center and Oklahoma City bombings. Also included are a number of less well-known attacks and thwarted attacks on facilities like electric power transformers and utility towers over the past decade. A much more significant aspect of this threat exists in the form of nuclear weapons. Reports from Russia suggest that some so-called "suitcase weapons" are unaccounted for and may have fallen into the hands of terrorists. Federal Bureau of Investigation (FBI) Director Louis Freeh recently testified that while there is no hard evidence to confirm these reports, they are being treated with utmost seriousness.[3] Increasing attention is also being focused on chemical, biological and radiological threats. Chemical agents have already been used by terrorists, in the 1995 Aum Shinrikyo gas attack in Tokyo. In addition, work done for the



[3] Testimony of FBI Director Louis J. Freeh before the House Committee on International Relations, October 1, 1997.

Commission by a national laboratory found there is a credible threat to the nation's water supply systems from biological and chemical agents.

The second category is electronic weapons designed to attack computer-based systems. Included here are radio-frequency devices that capture computer signals as they emanate from the equipment, and electromagnetic pulse and radio-frequency weapons that are intended to destabilize or destroy sensitive electronic components. We determined that weapons of the latter type are still in exploratory stages.

In examining physical threats, the Commission concentrated on two critical issues:

1) the targeting of key links and nodes whose destruction might ripple through infrastructures or across infrastructures, and

2) coordinated attacks which, in combination, could severely impact the nation's security and economic competitiveness.

Simulation exercises with senior representatives of the infrastructures and government shed some light on potential impacts of such attacks, but much more work is needed to understand the implications of interdependent infrastructures.

Cyber Threats

The Commission focused more on cyber issues than on physical issues, because cyber issues are new and not well understood. We concentrated on understanding the tools required to attack computer systems in order to shut them down or to gain access to steal, destroy, corrupt or manipulate computer data and code. In addition to accidents and negligence, threats to computer systems cover a broad spectrum that ranges from prankish hacking at the low end to organized, synchronized attacks at the high end. But the basic attack tools—computer, modem, telephone, and user-friendly hacker software—are common across the spectrum and widely available.

Potential cyber threats and associated risks range from recreational hackers to terrorists to national teams of information warfare specialists. Repeatedly identified as the most worrisome threat is the *insider*—someone legitimately authorized access to a system or network. Other malefactors may make use of insiders, such as organized crime or a terrorist group suborning a *willing* insider (a disgruntled employee, for example) or making use of an *unwitting* insider (by getting someone authorized network access to insert a disk containing hidden code, for example).

Five examples of new types of attack help illustrate the way commonplace cyber tools can be used to do harm.

A Cyber Attack on the Specific Data Base of an Owner/Operator

In the case of unauthorized entry into a network or system for the purpose of illegal financial transfers, stealing proprietary information, disrupting records, or merely "browsing," owners and operators have a responsibility for prudent and sufficient security systems such as firewalls and

passwords and qualified personnel to detect anomalies that indicate a successful entry so that further isolation or deflection measures can be taken to foil the attack.

A Cyber Attack for the Purpose of Gaining Access to a Network

If a particular system or network is discovered through "electronic reconnaissance" to have low security standards and to be interconnected to other networks of interest to the attacker, the attacker will use the most weakly defended pathway for access to the targeted system. This suggests that owners and operators need to consider establishing security standards for those with whom they are connected.

A Cyber Attack for the Purpose of Espionage

Intellectual property is vulnerable to theft in entirely new ways. The threat may come from a witting or unwitting insider, an unscrupulous competitor, or the intelligence service of a foreign power. Competitive advantage may be lost without knowing it was even at risk. This is true in business as well as in government.

A Cyber Attack for the Purpose of Shutting Down Service

Attacks by flooding communication lines have denied 911 service in some communities and shut down e-mail service to major users. Denial-of-service attacks are of concern to all institutions whose business depends on reliable communications. Sharing information about the tools used in these attacks and techniques to deflect or defeat them is therefore of interest to a wide range of public and private institutions.

A Cyber Attack for the Purpose of Introducing Harmful Instructions

An attacker can plant a virus or leave behind a program that will give the attacker critical information, such as passwords that can be used to log in to other networks. A virus may be transmitted within a local area network or passed on to an external net. "Logic Bombs" and "Trojan Horses" are designed, respectively, to destroy software at a preselected time and to enable future access. Given the rate of development of viruses, it is essential that all interconnected users adopt a high level of virus detection.

The Internet

Threats to the Internet are of primary concern because we are becoming increasingly dependent on it for communications—including government and military communications—for commerce, for remote control and monitoring of systems, and for a host of other uses; because our ability to understand its full impact on society seems unable thus far to keep up with its explosive growth; and because it is inherently insecure (see Figure 2).

The Internet was designed in 1968 by the then Advanced Research Projects Agency (ARPA), now the Defense Advanced Research Projects Agency (DARPA), to determine how to build resilient computer networks that could survive physical attacks or malfunctions in portions of the

network. The ARPAnet, as it was called, was not designed as a secure network, but depended for security on a small number of users who generally knew and trusted one another.

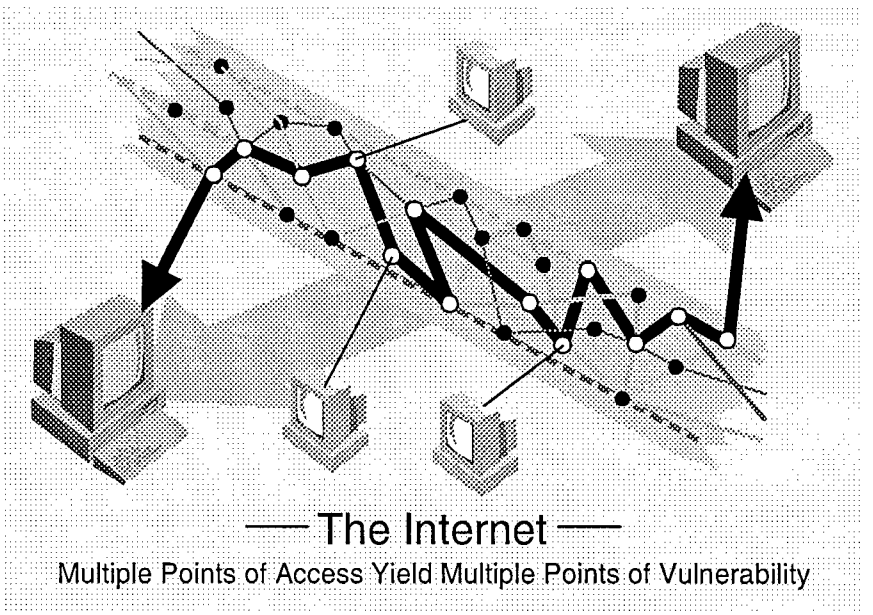


Figure 2. Increasing Exposure

Commercialization of the Internet in the early 1990s, boosted by the WWW, caused incredible growth. Government and the private sector began to seize the advantages of the Internet as an alternative to other unclassified means of communication. The Internet continues to proliferate globally. In general our growing proclivity to network continues to outpace network protection. The price for the efficiency of networking is increased exposure of data and systems to unauthorized and anonymous access. A study done for the Commission by Carnegie-Mellon University's Computer Emergency Response Team (CERT) confirmed that "because the ties between critical infrastructures and the Internet will continue to become stronger and more intricate, the impact of an Internet attack could be devastating."[4]

Information Warfare

Even more recent than the evolution of the Internet has been development and open discussion of the concept of Information Warfare (IW). The Gulf War illustrated the importance of infrastructures to national defense—our domination of Iraq's information and communications ensured victory over a well-armed military force with minimum allied losses. Other nations have drawn similar conclusions. Offensive IW, in brief, uses computer intrusion techniques and other capabilities against an adversary's information-based infrastructures. The Commission is aware of little in the way of special equipment required to launch IW attacks on our computer systems; the basic attack tools—computer, modem, telephone, and software—are essentially the same as those used by hackers and criminals. And compared to the military forces and weapons that in the past threatened our infrastructures, IW tools are cheap and readily available (see Figure 3).

If the basic cyber attack tools and skills are common across the spectrum, what may distinguish recreational hackers from Information Warriors is ***organization***. Said another way,

[4] CERT report to the Commission, January 1997, p. 3.

an IW attack against US infrastructures may be little more than a series of hacker attacks, conducted against carefully chosen and thoroughly reconnoitered targets, synchronized in time, to accomplish specific purposes.

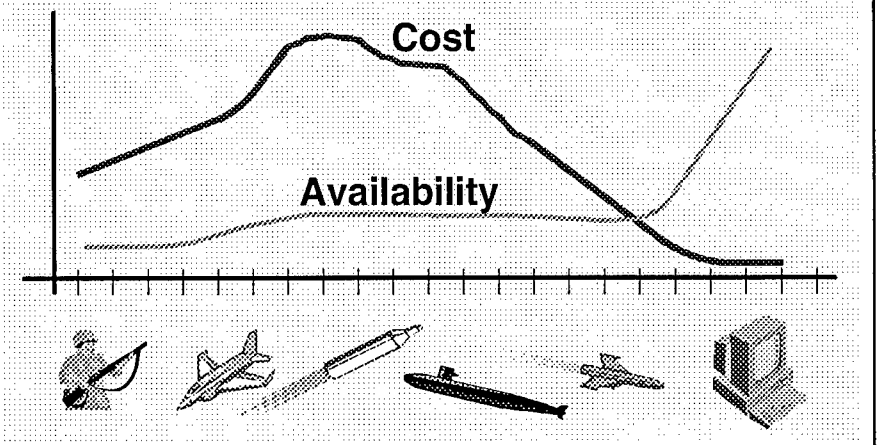


Figure 3. Tools to Do Harm

For an adversary willing to take greater risks, cyber attacks could be combined with physical attacks, against facilities or against human targets, in an effort to paralyze or panic large segments of society, damage our capability to respond to incidents (by disabling the 911 system or emergency communications, for example), hamper our ability to deploy conventional military forces, and otherwise limit the freedom of action of our national leadership.

Terrorists frequently choose prominent targets that produce little physical impact beyond the target itself, but widespread psychological impact. For a physical attack on infrastructures, less spectacular targets could be chosen, such as switching stations, communications antennas, pipelines, transformers, pumping stations, and underground cables. Many facilities whose physical damage or destruction would have a disruptive effect on an infrastructure are purposely located in sparsely populated or even unpopulated areas. If they are physically attacked it may take some time to discover the nature of the damage, and in the absence of casualties it may be some time before the attacks are reported. Even when they are reported, each incident is at first a local event, and if several such events occur over a period of weeks or months it may take considerable time before they are recognized as part of a pattern. Recognition that an attack is in progress could be delayed even if physical attacks were to occur simultaneously, if the targets were spread across several jurisdictions and no mass casualties were produced to generate "breaking news" at the national level.

The chances of immediately discovering that a concerted cyber attack is in progress are today even slimmer. Computer intrusions do not announce their presence the way a bomb does. Depending on the skill of the intruder and the technology and training available to their own system administrators, individual companies whose networks are penetrated may or may not detect an intrusion. Intrusions that are discovered may or may not be reported to law enforcement authorities, who may or may not have the resources to investigate them and conclude whether they are the work of an insider, a hacker, a criminal, or someone truly bent on harming the infrastructure. It sometimes takes months, even years, to determine the significance of individual computer attacks. In the highly publicized 1994 Rome Labs case, the main intruder—a London teenager—was caught in the act; but his alleged accomplice and mentor—who turned out to be a

Welsh computer specialist only a couple of years older—was not identified and arrested until more than two years later.

In the absence of intrusion detection tools, uniform reporting of incidents as they occur, and some central capability to analyze incidents as they are reported, it is conceivable that an orchestrated attack against US infrastructures could be under way for some time before it is recognized as such and the attacker's motives and objectives can be deduced.

Intelligence Community Challenges

Information Warfare presents significantly new challenges for the intelligence community in identifying and assessing threats to the United States. This is partly because concepts of IW are only now taking shape abroad and because tools and techniques used for IW attack are inexpensive and ubiquitous. It is clear that a number of nation-states are closely following US developments in IW and are themselves exploring IW capabilities. They recognize that modern industrialized states are increasingly dependent on the uninterrupted flow of information. In addition, sub-national groups increasingly rely on advanced information technologies to support their illegal operations, and US intelligence analysts must be on the look-out for indications of interest by these groups in using their technical knowledge to harm the United States by attacking our critical infrastructures.

Recent assessments of foreign IW threats suggest a measured apprehension about the future. While no one is forecasting a sudden and major IW attack on the United States in the next few years, a number of factors support the sense of a growing threat. The US is by no means alone in recognizing and seizing the advantages of the global information and communications infrastructure and thus the increasing likelihood of various forms of international competition in the information arena. It is reasonable to assume that the number of states following our lead will increase. Other states and non-state groups will become increasingly familiar with opportunities for offensive use of computer techniques as they develop their own technology base and necessary cyber defensive capabilities. Finally, computer crime, including that directed against American businesses, will continue to grow in nation-states that do not enforce strong prosecution.

Shared Responsibility

The government and private sector share substantially the same national information infrastructure. Both have been victims of unauthorized computer intrusions, theft, and disruption. In our view, the line separating threats that apply only to the private sector from those associated with traditional national security concerns must give way to a concept of shared threats (see Figure 4). Shared threats demands a shared response, built from increased partnership between government and the owners and operators of our infrastructures.

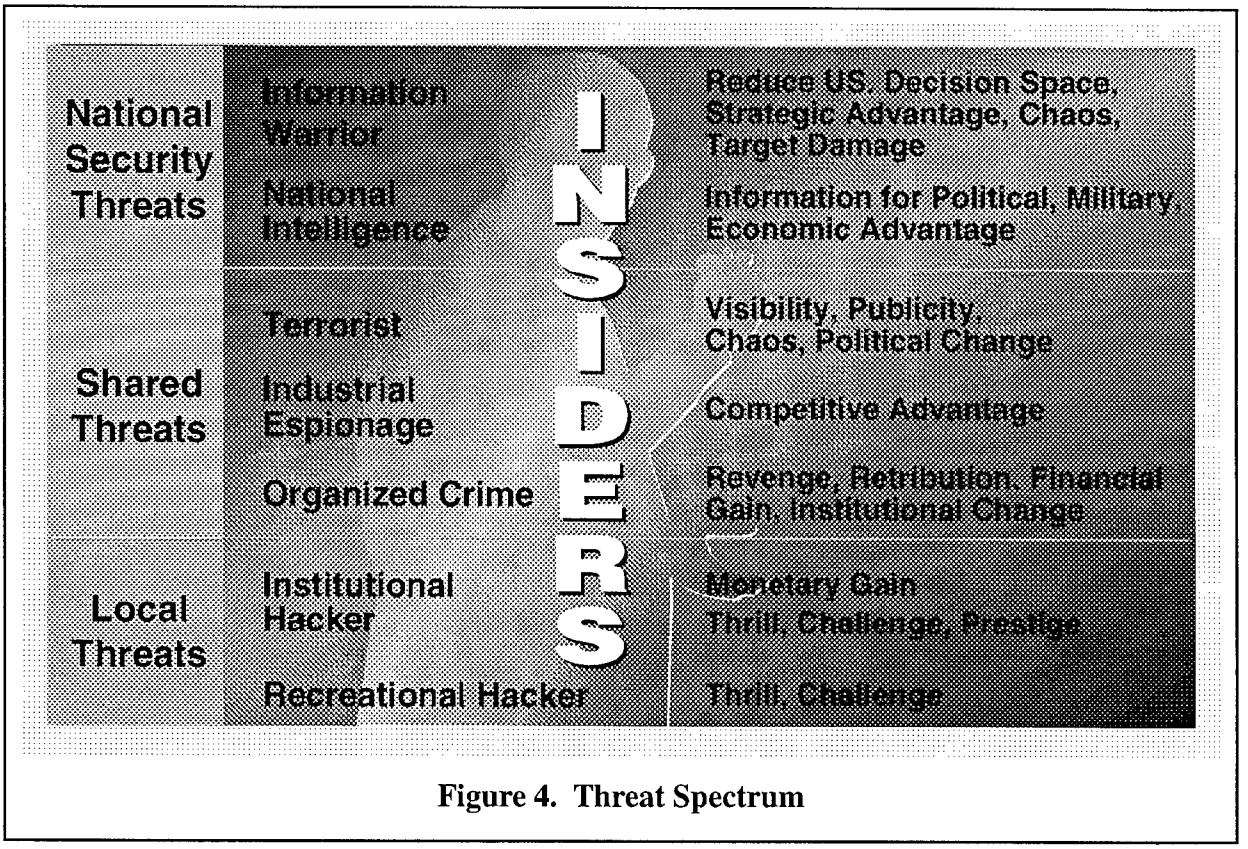


Figure 4. Threat Spectrum

Factory owners or service providers were not expected in the past to protect themselves from enemy bombers or missiles; that was government's job. In the future, though, the owners and operators may be on the front line, and their networks may be the battlefield. The tools and know-how required to do harm are inexpensive, readily available, and easy to use.

Owners and operators need to protect themselves from the tools and the know-how. Government can help by collecting and disseminating information about all the tools that can do harm. Owners and operators can help by informing government when new tools or techniques are detected. Government has an obligation to collect information about potentially hostile groups and nation-states, and to issue timely warnings alerting owners and operators when new threats are detected.

We must achieve a new understanding of the threats that confront us—an understanding that focuses on the capability to do harm rather than identifying the person, group or nation intent on doing harm. Traditional indicators of developing capability are not present. There are no missile silos to count or railway cars to examine. We must acknowledge that the capacity for harm exists, and act now, as partners, to protect our future.

Chapter Four

Findings and Policy

Analysis of the infrastructures, their vulnerabilities, and shared threats led the Commission to several observations. This chapter sets out those findings and then suggests a policy framework that addresses them. Subsequent chapters deal with specific recommendations resulting from that process.

In some respects our most important finding was the need to think differently about infrastructure protection. The management approach we now use was designed to deal with the Industrial Revolution, then was adjusted to manage successively the stabilization of America after the Civil War, the Depression, World War II, and finally the nuclear stand-off of the Cold War. None of those approaches is particularly applicable to the world as it will look through the lens of information technology in the third millennium.

FINDING: **Information sharing is the most immediate need.**

There are many instances in which information is shared between the private sector and government, as in the case of the North American Electric Reliability Council (NERC) and the Presidentially-appointed National Security Telecommunications Advisory Committee (NSTAC). But there are important shortfalls. Increasing the sharing of strategic information within each infrastructure, across different sectors, and between sectors and the government will greatly assist efforts of owners and operators to identify their vulnerabilities and acquire tools needed for protection.

FINDING: **Responsibility is shared among owners and operators and the government.**[5]

[5] While sometimes these owners and operators are referred to as the "private sector," in truth the infrastructures also include publicly-owned and operated activities such as municipal water companies, state and local highway departments, and fire, police, and emergency response agencies.

Owners and operators have always focused on protecting themselves from known threats to their operations, because it is in their interest. The government has always focused on protecting the nation from threats beyond the capabilities of private self-protection. Today, an adversary can bypass our national defense forces to attack directly the infrastructures that underpin our national economic strength. Traditional national security concerns must give way to a concept of shared threats, for which responsibility must be shared between government and infrastructure owners and operators.

FINDING: **Infrastructure protection requires integrated capabilities of diverse federal agencies, and special means for coordinating federal response to ensure these capabilities are melded together effectively.**

The Commission believes that the federal government's job in infrastructure protection includes the traditional defense, law enforcement, intelligence, and other responsibilities as well as the additional effort, resources and processes to respond to the cyber dimension. The structures detailed in our recommendations are designed to expand the reach of existing capabilities, provide a means to coordinate them, and integrate them with the resources of the owners and operators.

FINDING: **The challenge is one of adapting to a changing culture.**

Our culture is changing at an accelerating pace. The Information Age is still unfolding, but it is already clear that it brings with it at least as many adjustments to our way of life as did the Industrial or the Nuclear Age, and that the requirement to adapt will be more urgent. Bold, sweeping measures are required to educate and inform our private sector, public servants, and citizens about the realities of the new environment.

FINDING: **The federal government has important roles in the new infrastructure protection alliance with industry and state and local governments.**

The federal government is in a position to lead by example by adopting best practices, actively managing risk, and improving security planning in its own systems.

FINDING: **The existing legal framework is imperfectly attuned to deal with cyber threats.**

Laws change at a much slower rate than technology. The existing legal framework does not reflect current technology in a number of ways. Legal authorities will need to be modified to allow for greater awareness of information security concerns, to enable response to and recovery from cyber events, to increase deterrence against computer crimes domestically and internationally, and to clarify roles and responsibilities in a world that is increasingly moving away from jurisdictional boundaries.

FINDING: **Research and development are not presently adequate to support infrastructure protection.**

New challenges require new resources and new examination of how to protect ourselves. The Commission's proposed research and development (R&D) program identifies specific areas for research to provide the needed technologies.

Toward Recommendations

As we approached making recommendations to assure our critical infrastructures, the Commission adopted a set of principles to guide our decisions.

- ***Build on that which exists.*** It will be easier and faster to implement, more effective, and more likely to be accepted than creating something new.
- ***Depend on voluntary cooperation.*** Partnerships between industry and government will be more effective and efficient than legislation or regulation.
- ***Start with the owners and operators.*** They have a strong economic stake in protecting their assets and maximizing customer satisfaction. They understand the infrastructures and have experience in responding to outages.
- ***Practice continuous improvement.*** Take action in affordable increments. There is no "magic bullet" solution. Aim not only to protect the infrastructures, but also to enhance them.
- ***Coordinate security with maintenance and upgrades.*** Security should be incorporated in planned maintenance and scheduled upgrades.
- ***Promote government leadership by example.*** Government-owned facilities should be among the first to adopt best practices, active risk management, and improved security planning.
- ***Minimize changes to government oversight and regulation.*** Several of the infrastructures have a long history of government regulation, with a clear legislative mandate and a record of success. We consciously avoided proposing significant changes in regulation.

A Proposed National Policy for Infrastructure Protection

Critical infrastructures underpin the security of our national wealth, our defense capability, the economic prosperity of the people, and, above all, the maintenance of the system of human rights and individual freedoms for which the United States was founded and has stood since 1776. The threat of infrastructure attacks therefore has the potential for strategic damage to the United States. Accordingly, the assurance of critical infrastructures deserves national attention and leadership by the federal government.

It shall be the policy of the US to assure the availability and continuity of the critical infrastructures on which our economic security, defense, and standard of living depend. The infrastructures will be defended by whatever means necessary, including the full range of business, legal, law enforcement, military, and social tools available.

Further, the US recognizes that assuring infrastructure is not just a government or business responsibility, but is shared by those public and private interests that own and operate the infrastructures and the government agencies responsible for defense, law enforcement, and economic security of the nation.

The interdependent nature of the critical infrastructures and their collective dependence on the information and communications infrastructure have created new assurance challenges that can only be met by a partnership between owners and operators and government at all levels. Only the owners and operators have the knowledge, access, and technology to defend their systems from the growing array of widely available information-based tools. Only the federal government has the legal authority, law enforcement capability, and defense and intelligence resources needed to deter the most sophisticated nation-state and other serious cyber threats. And only the federal government has the intelligence and related capabilities to find the tools that do harm and promulgate information about them throughout the infrastructures.

As a matter of urgency, an Office of National Infrastructure Assurance should be established under the National Security Council (NSC) and given overall program responsibility for infrastructure assurance matters, including policy implementation, strategy development, federal interagency coordination, and liaison with state and local governments and the private sector. Among other responsibilities, this Office will devise and establish mechanisms for the exchange of views and information between the government and the private sector, identify information requirements for infrastructure assurance, and ensure that infrastructure assurance considerations are taken into account in making other government program decisions.

The Office of National Infrastructure Assurance should ensure that a program of public awareness is implemented throughout the country to inform the American public about infrastructure protection. This will include establishment of appropriate curricula in the national education system, from kindergarten through graduate school and including professional training. The Office of National Infrastructure Assurance should also ensure that individual agencies of the federal government implement infrastructure preparedness provisions and update their security plans to include protection against Information Warfare threats.

Part Two

A Strategy for Action

(Intentionally Left Blank)

Chapter Five

Establishing the Partnership

Information Sharing—The Indispensable Step

Objective

Promote a partnership between government and infrastructure owners and operators beginning with increased sharing of information relating to infrastructure threats, vulnerabilities, and interdependencies.

Need for Sharing Information About the Cyber Dimension

The private sector owners and operators of critical infrastructures are engaged in market-based programs offering services at competitive prices. Their risk analysis weighs the cost of physical and cyber disruption against the cost of physical and cyber security. Their willingness to invest in defenses against the cyber tools that may do harm is dependent on their experience with these disruptions and the information they have about them.

While physical security is a mature discipline, our understanding of cyber vulnerabilities and threats is incomplete. Owners and operators do not have sufficient threat and vulnerability information for informed risk management decisions. Some of the information they need may be available from the federal government, particularly from the law enforcement and intelligence communities.

As emphasized earlier, two-way sharing information is indispensable to infrastructure assurance. While infrastructure owners and operators have the fullest appreciation of vulnerabilities, they have access only to their own information or, in some cases, information pertaining to their industry or sector. Consequently, there is no comprehensive body of knowledge available for effective analysis of overall infrastructure vulnerabilities and threats. This is especially true of vulnerabilities created by increased dependence of infrastructures on one another. Current

information-sharing mechanisms perform well in matching physical threats to known vulnerabilities, and employing appropriate countermeasures. However, the same cannot be said of the emerging cyber arena.

Overcoming Reluctance

Our contacts with public and private sector stakeholders identified a need to increase the flow of information about cyber threats and vulnerabilities. Many offered a perception that private sector owners and operators share information only when they suffer substantial loss or are convinced of imminent danger to continuity of operations.

Infrastructure representatives expressed reluctance to share information about vulnerabilities because they fear it might be made public, resulting in damage to their reputations, exposing them to liability, or weakening their competitive position. Many also feared that sharing vulnerability information could invite unwanted federal regulation. The degree of reluctance varied according to infrastructure, but was present in each. The latest Computer Security Institute/FBI Computer Crime and Security Survey reinforces these observations, noting that of respondents who experienced an attack during the previous year, only 17 percent reported it to law enforcement authorities.[6]

Owners and operators told us they might have a better idea of actions they should take if the government shared more threat and vulnerability information. Likewise, government representatives told us they could better protect infrastructures if owners and operators would stop withholding information. While it is clear that government and the private sector would benefit from an improved two-way flow of information concerning threats and vulnerabilities, we caution against expecting a sudden revelation. Our classified government briefings and confidential discussions with private sector representatives produced no evidence of some missing piece of information that would make the whole picture suddenly fall into place.

Need for National Analytic Capability

Of course, sharing information isn't enough; we need the analytic tools to examine information about intrusions, crime, and vulnerabilities and *determine what is actually going on in the nation's infrastructures*. Deciding whether a set of cyber and physical events is coincidence, criminal activity, or a coordinated attack is not a trivial problem (see Figure 5). In fact, without a central information repository and analytic capability, it is virtually impossible to make such assessments until after the fact. This is of increasing concern as infrastructure operations become more reliant on information and communications—the very sector about which it is most difficult to make assessments.

[6] Computer Security Issues & Trends, Vol. III, 1997 Computer Security Institute/FBI Computer Crime and Security Survey.

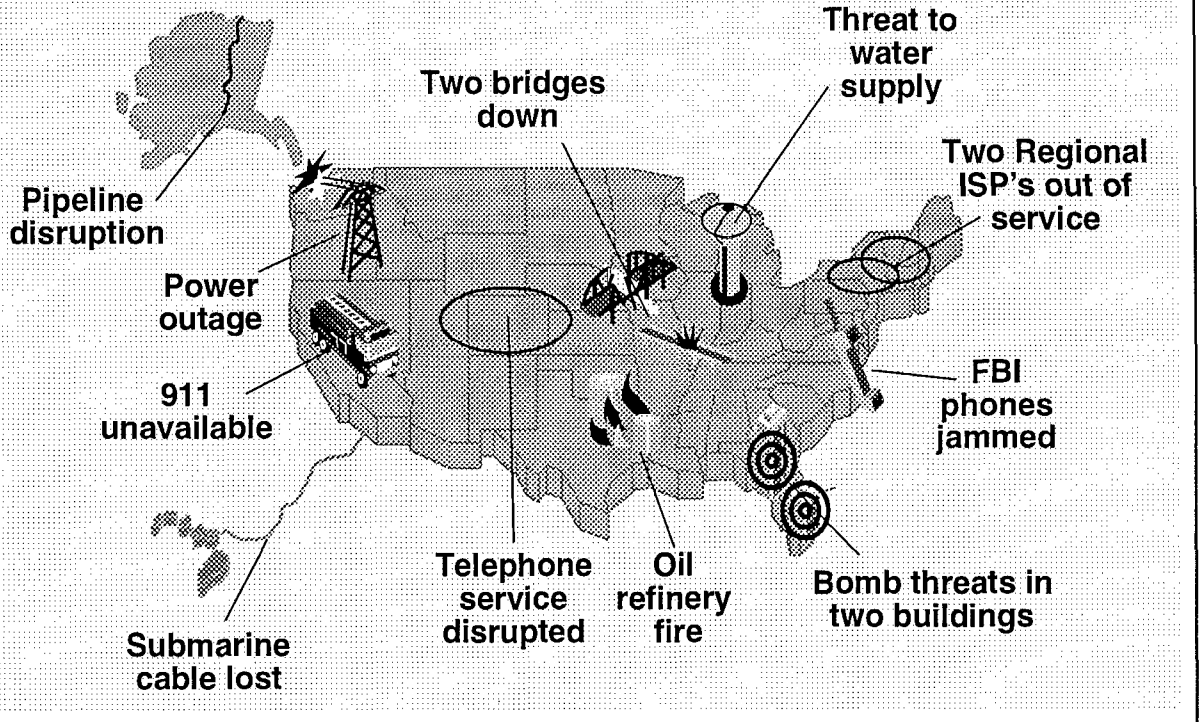


Figure 5. Coincidence or Attack?

A number of government and private organizations hold and distribute incident reports related to infrastructure protection, but comprehensive analysis of this information is limited. The need for analysis is especially critical to support decision-making about responding to attacks. There is insufficient interagency, federal-to-state and local government, or public/private correlation of data to support crisis action planning in response to a cyber terrorist incident. The need for "a cyber-threat-clearinghouse ... centralized effort for comprehensive intelligence analysis of cyber issues ... an industry/government information exchange for threat and vulnerability data" has been documented frequently.[7]

Existing Information Sharing Efforts

Our work did identify highly successful information sharing organizations already at work in other areas. The Centers for Disease Control and the Coordinating Sub-Group on Counter-Terrorism (CSG/CT) in the NSC are useful models for expeditious information sharing to support action planning.

[7] See, for example, The Future of US Intelligence, report by The Working Group for Intelligence Reform, 1996; NII Risk Assessment: A Nation's Information at Risk, report by the Reliability and Vulnerability Working Group, 1995; and NII: the Federal Role, report of the National Information Infrastructure Security Issues Forum, 1995. More details are contained in an internal Commission paper on Information Sharing.

We also found a great deal of information sharing already underway. Trade associations, consortia, and other groups exchange information among their members and, in some cases, directly with government. Many federal, state and local government agencies have existing relationships with infrastructure owners and operators. Within all the infrastructure sectors, at least some portions are subject to regulatory control by government agencies, and information is shared, albeit sometimes within carefully defined constraints.

Several federal agencies provide information to infrastructure owners and operators. The FBI's Awareness of National Security Issues and Response (ANSIR) program gives over 25,000 industry members information that provides threat and vulnerability insights. More narrowly focused programs are the Department of Transportation's terrorist threat notification to the civil aviation industry and the National Security Agency's INFOSEC Vulnerability Assessment Program, which provides information systems-related data to private sector partners. The Comptroller of the Currency operates another system providing advisories on information integrity and security risks to financial institutions.

Information To Be Shared

Common to most of these programs is the narrow range of information collected and shared. In almost every case, they are tightly focused on specific information with no attempt to determine whether the information might also be useful for infrastructure protection purposes. Regulatory information is not generally focused on infrastructure protection. For example, telecommunications carriers report service disruptions of 30 minutes affecting 30,000 or more customers to the Federal Communications Commission (FCC). But that reporting channel would not identify a series of smaller attacks dispersed around the country and designed to slowly weaken public confidence in the system.

Figure 6 depicts the types of information pertinent to infrastructure assurance and the likelihood that the information is reported to law enforcement. Currently, only information derived from selected threats and difficult-to-ignore, successful attacks is readily shared. This narrow range of reported types of information should be viewed as only the tip of a mountain of data whose compilation would be helpful in infrastructure

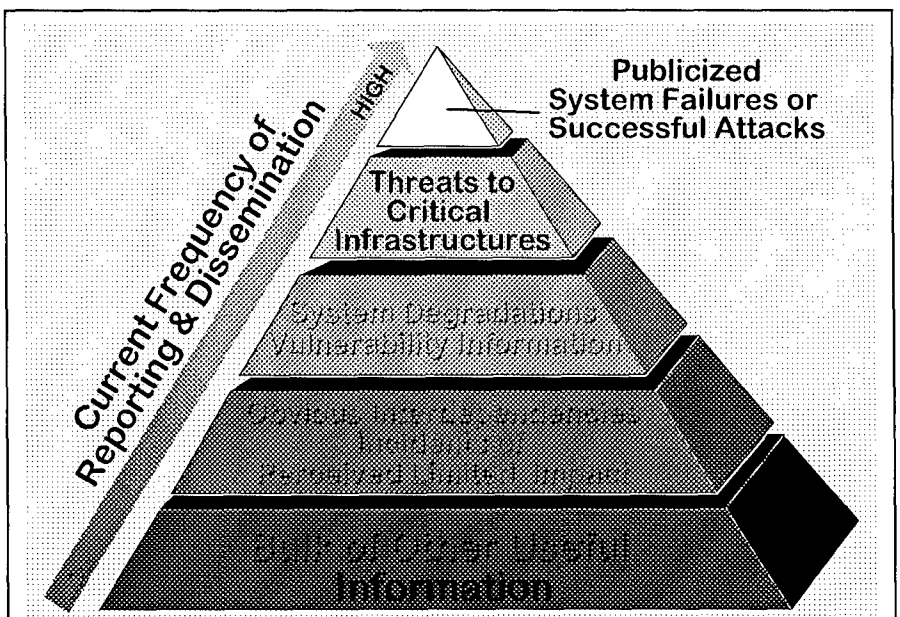


Figure 6. Scope of Useful But Unavailable Information

assurance. Included are such topics as system degradations due to physical acts or cyber-based events; vulnerabilities (hardware failure rates, operator-induced malfunctions, poor maintenance practices, or software flaws); not-so-obvious cyber or physical vulnerabilities resulting from dependence on other infrastructures; incidents of vandalism, malicious mischief, or suspicious activity; and physical or cyber anomalies. Information in government hands, such as criminal statistics and threat data, seldom is scrutinized for revelations about vulnerabilities or interdependencies. The government and infrastructure owners and operators must both push assurance-related data from the bottom towards the top of their respective agendas where it can be more readily analyzed.

Legal Impediments to Information Sharing

We envision the creation of a trusted environment that would allow the government and private sector to share sensitive information openly and voluntarily. Success will depend on the ability to protect as well as disseminate needed information. We propose altering several legal provisions that appear to inhibit protection and thus discourage participation.

Confidential Information

The Freedom of Information Act (FOIA) makes information in the possession of the federal government available to the public on request. Potential participants in an information sharing mechanism may require assurances that their sensitive information will remain confidential if shared with the federal government.

We Recommend:	The proposed Office of National Infrastructure Assurance require appropriate protection of specific private-sector information. This might require, for example, inclusion of a b(3) FOIA exemption in enabling legislation.

Trade Secrets and Proprietary Information

Private sector participants may be reluctant to share sensitive information if appropriate protection mechanisms are not incorporated.

We Recommend:	The proposed Office of National Infrastructure Assurance require appropriate protection of information containing trade secrets or other forms of proprietary information.

Classified Information

Information collected by the government to benefit a threat warning process may require protection in the form of classification.

We Recommend:	The proposed Office of National Infrastructure Assurance consider the need for classification of certain information, or certain bodies of aggregated information, and the impact that classification would have on the dissemination process.

Antitrust

Potential contributors from the private sector are reluctant to share specific threat and vulnerability information because of impediments they perceive to arise from antitrust and unfair business practice laws.

We Recommend:	The Department of Justice (DOJ) offer limited assurances to the private sector that participation in information sharing processes would not run afoul of antitrust laws and consider providing appropriate guidelines to inform participation.

Liability

Information which could prevent harm to a critical infrastructure may arise from participation in a threat and warning capability. Failure to share such information, or to act on such information shared by others, might carry liability consequences for public and private participants.

We Recommend:	The federal government undertake a detailed study of liability issues surrounding participation in an information sharing process.

National Security

Currently, many federal agencies have their own specific guidelines controlling interaction with foreign corporations or corporate entities with significant foreign ownership.

We Recommend:	The NSC study whether the federal government should standardize guidelines for sharing infrastructure assurance information with foreign corporations in light of potential national security risks and benefits.

Appropriate guidelines are needed for sharing information with foreign corporations.

We Recommend:	In the short term, the proposed Office of National Infrastructure Assurance set guidelines for the sharing of infrastructure assurance information with foreign corporations.

State Government Liability and Disclosure

Many of the legal impediments to information sharing identified at the federal level exist at the state level as well. However, diversity among state laws further complicates efforts to maximize participation in information sharing.

We Recommend:	A study group identify legal impediments to information sharing at the state level, propose solutions, and draft model legislation.

Conclusion

We believe information sharing is the critical foundation for an effective partnership to enhance our ability to protect critical infrastructures in the years ahead. Sharing information figures prominently in the additional recommendations we make and the structures we recommend for the public and private sector elsewhere in this report. How then should we build the relationship between private and public sector organizations so they can share, use, and act on information to better protect our critical infrastructures?

(Intentionally Left Blank)

Chapter Six

Building the Partnership

Owners and Operators
State and Local Governments

Objective

Ensure infrastructure owners and operators and state and local governments are sufficiently informed and supported to accomplish their infrastructure protection roles.

Protecting America's infrastructures is neither an entirely public nor entirely private interest. Vulnerabilities pose risks to government, business, and citizen alike. Reducing those risks requires coordinated effort within and between the private and public sectors. The need for infrastructure protection creates a zone of shared responsibility and potential cooperation for industry and government.

Owners and operators have a responsibility to deliver reliable service. While sometimes these owners and operators are referred to as the "private sector," in truth the infrastructures include publicly-owned and operated entities such as municipal water companies, state and local highway departments, and fire, police, and emergency response agencies. Regardless of whether they are primarily accountable to shareholders or taxpayers, owners and operators must take prudent steps to reduce or eliminate their own vulnerabilities—*to protect themselves not so much against a known threat, but against the tools an unknown perpetrator could employ.*

Government has an undeniable role in accomplishing the tasks that government alone can undertake—including law enforcement at local, state and federal levels, and national intelligence, defense and diplomacy.

The Commission found a need for a new partnership between government and owners and operators to assure our critical infrastructures. And we found that the need to share information was a foundation on which we could build that partnership.

Infrastructure assurance is essentially a process of risk management. The process is generally defined to include prevention, mitigation, incident management, and recovery. The many functions associated with infrastructure assurance fit into these four categories.

In considering how these functions are accomplished today, and how they might be in the future, we identified opportunities for enhancing the effectiveness of the owner and operators through increased partnership with the federal government.

National Threats and Public-Private Partnerships

Our approach to partnership for infrastructure assurance was to examine which functions were the responsibility of each partner and the expectations associated with those functions. This led to the specific recommendations contained in this discussion about private sector, and state and local government roles.

A New and Challenging Environment

Infrastructure providers deal with known vulnerabilities and associated risks within their infrastructures. But the rapid introduction of new technologies and interconnected nature of the infrastructures present new challenges. Before interdependencies were as great as they are now, physical attacks and outages were contained. Extensive reliance on computer and telecommunications technologies makes it more difficult for owners and operators to know whether outages result from technical failure or intentional intrusion.

Further complicating the partnership is our dependence on these infrastructures for national defense, economic competitiveness, and quality of life. Realizing this certainly places the role of critical infrastructure owners and operators into new perspective. While they must still respond to normal business pressures—the bottom line, shareholder concerns, and their customers—they must also acknowledge that the government has an increasing interest in infrastructure providers. The critical role of many public utilities exemplifies this situation where health, safety and other public concerns are so dependent on the infrastructure that government interest is unquestioned. Today, the interconnected nature of the infrastructures, the potential for local disruptions to cascade into other infrastructures, and the dependence of national security on those same infrastructures present a clear need to think in new ways.

These facts alone emphasize the need for infrastructure owners and operators and government at all levels to find new ways of working together. These new partnerships must be designed to

foster mutual trust and facilitate sharing of the types of information that each partner needs to assure the uninterrupted flow of essential goods and services.

Expectations of Owners and Operators[8]

Owners and operators are the primary players in infrastructure assurance. For all the expected business and operational reasons, they protect their critical systems and facilities based on a perceived set of risks. Better information on emerging threats and vulnerabilities, particularly those stemming from unrecognized or little understood interdependencies, will assist managers in making decisions about investment in security processes, thus improving assurance not only for their own company's operations, but for operation of the infrastructure overall.

The Commission believes it is the responsibility of owners and operators to:

1) Provide and manage facilities delivering services to customers efficiently and effectively.

2) Meet customer expectations for quality and reliability of service.

3) Maintain an effective risk management process adequate to:
   - identify vulnerabilities and potential threats that might affect continuity of service;
   - prevent and mitigate as many credible threats as economically feasible; and
   - maintain emergency response capability to quickly restore service and eventually reconstitute the infrastructure in the event of service interruptions.

4) Give special consideration to the vulnerabilities currently in many information systems.

5) Cooperate within their industry to identify best practices for improving service reliability and security.

6) Report possible criminal activities to law enforcement agencies and cooperate with investigations.

7) Establish a relationship with intelligence and law enforcement to assure that information about warnings and threats is communicated in a timely way and that the industry experience with incidents is available as an input to threat analysis.

[8] As previously noted, the term "infrastructure owners and operators" includes public agencies or corporations as well as companies and activities in the private sector.

Risk Assessment Best Practices

Conduct a security training program for all employees according to their job responsibilities and access authorizations, integrating this program with existing physical security aspects.

Authenticate the identity of all users of the system, determine the uses of the system for which they are authorized, and restrict access to only the authorized functions and data.

Isolate critical operational control systems from all public and most internal networks, or provide adequate firewalls.

Provide adequate procedural and technical controls to assure data integrity, to detect instances of unauthorized change or deletion, and to recover when necessary.

Authenticate and log the origin of all commands to change the operating conditions of the controlled infrastructure.

Create a CERT, or similar response capability, with the equipment and training needed to investigate suspected intrusions, isolate and recover damaged systems, and restore service to customers.

Provide adequate back-up and recovery capability for the programs and data of any information system that is necessary for normal operations and customer service. To better assure the availability of key control systems, information systems and data, consider redundancy, geographic separation of primary and back-up systems, alternative methods, effective use of encryption, and other relevant security options.

Conduct regular assessments of the vulnerability of information systems using the technical expertise of the National Security Agency (NSA) and others as appropriate to assure that new techniques for attacking systems can be contained by the protective measures currently installed.

Compiled by the President's Commission on Critical Infrastructure Protection

Industry Suppliers

Usually the owners and operators are not the suppliers of the computer hardware and software they use to manage their operations. For significant improvements to be made in the security and integrity of these information systems, suppliers must be involved.

The computing systems industry is highly competitive and normally very responsive to customer needs; however, experience suggests that users may not understand the new vulnerabilities well enough to demand products offering better security. There is recent evidence that major suppliers are giving security and integrity more attention than in the past. We expect this trend to accelerate as owners, operators, and industry associations study their vulnerabilities and demand improved products.

Vulnerabilities Assessments

The more owners and operators understand about their vulnerabilities (see Figure 7), the better able they are to make effective decisions about protecting their operations. A step toward increasing private sector awareness can be taken by increasing federal government participation in the vulnerability assessments conducted by owners and operators.

We Recommend:	The NSA, the Department of Energy (DOE) and DoD: • continue to perform vulnerability assessments for critical infrastructure owners and operators. • provide vulnerability assessment training to private sector service providers on a cost-reimbursable basis, e.g. sharing knowledge and expertise of key government centers of excellence.

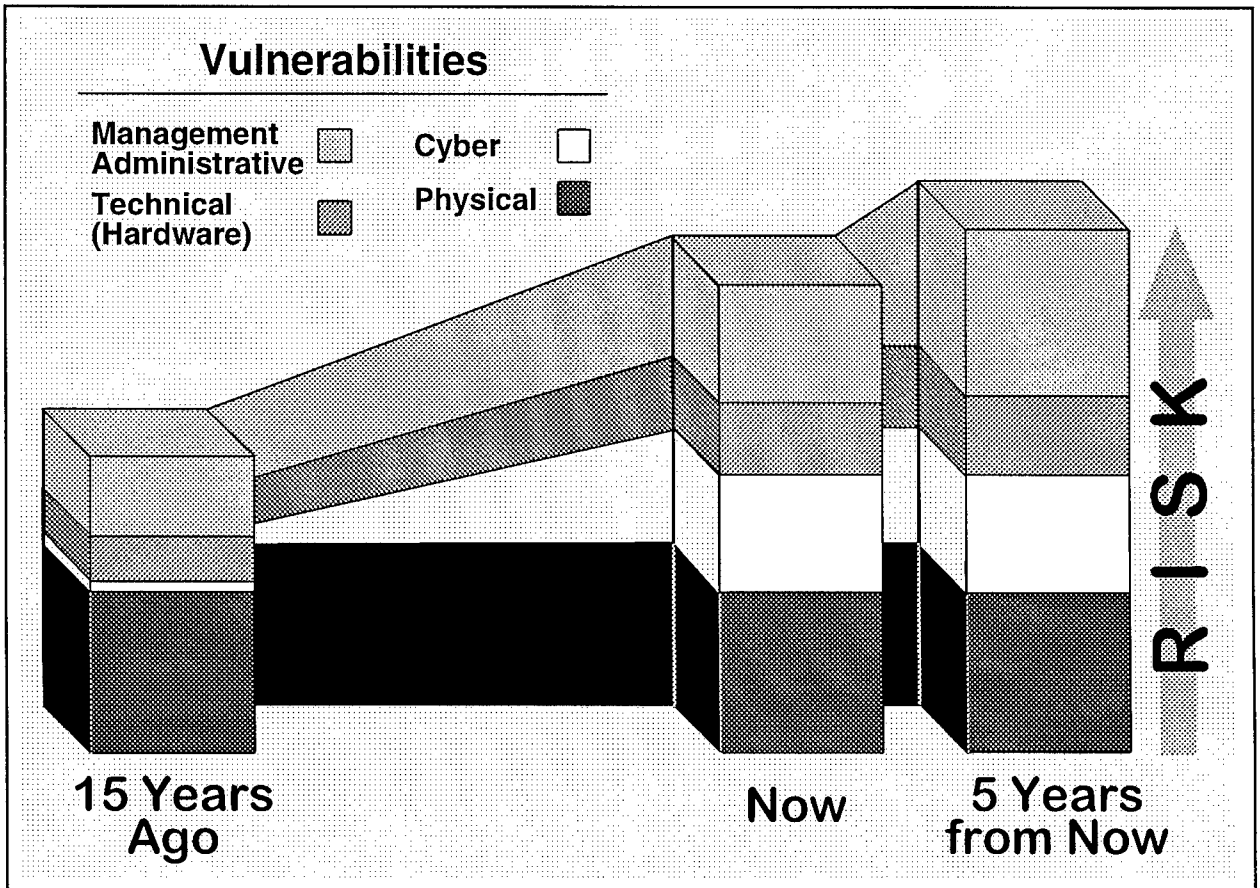


Figure 7. Vulnerabilities Profile

Publicize & Support Application Of Risk Assessment Methodologies

We Recommend:	The proposed Office of National Infrastructure Assurance and National Infrastructure Assurance Council encourage private industry to perform periodic risk assessments of critical processes, including information and telecommunications systems. This will enable more informed risk management decisions in the face of rapid, pervasive change.

We Recommend:	The proposed Office of National Infrastructure Assurance encourage the insurance industry to develop its risk methodologies for application to the critical infrastructure industries.

Sensitive Information

In Chapter 5, we described the need to overcome the concern of owners and operators that information they provide to government might not be protected. As the importance of the infrastructures to every aspect of national strength is understood, information that may be useful to an enemy in designing an attack on those infrastructures takes on a new importance.

One example of concern in this area is found in requirements for publication of sensitive information about critical components or the functioning of infrastructures. This information has the potential to serve as a "road map" for a potential infrastructure attack; therefore, its publication may lead to the exploitation of vulnerabilities.

We Recommend:	The President issue an Executive Order requiring that federal agencies accomplish the following before publishing or requiring the publication of information about critical components or functioning of infrastructures. • bring together the relevant stakeholders to discuss the implications of the requirement. • identify the purpose for publishing the information and ensure that the information is published in a format that minimizes the likelihood it will be used in ways that are incompatible with infrastructure assurance. • certify that the positive and negative effects on infrastructure assurance have been fully explored, including that the potential benefits of publication outweigh any identified risks.

Protection of Infrastructure Vulnerability Information

We now must question whether information regarding vulnerabilities—in the aggregate at least—shouldn't be protected in some fashion.

We Recommend:	The US Security Policy Board be tasked to provide a recommendation to the President on criteria for and means of protecting otherwise unclassified private sector information on threats and vulnerabilities to critical infrastructures.

Publication of Infrastructure Assurance Data

The publication of infrastructure assurance-related comparative data within an industry may positively influence performance by motivating increased attention to information security, as well as reliability, without resorting to regulation. This information may prove useful to consumers in light of increased competition and choice between providers of critical infrastructure services. We found such reports of great use in some infrastructures. In electric power, for example, the NERC publishes each month on its WWW site a Performance Honor Roll of companies achieving 95 percent or better reliability in the previous 12 months.

We Recommend:	The Administration direct the FCC's Network Reliability and Interoperability Council to initiate a feasibility study of publishing comparative infrastructure assurance-related data for the telecommunications industry. The study should focus on whether publication is likely to achieve infrastructure assurance objectives, the types of data to collect and publish, whether current data collection efforts are sufficient, and other possible impacts of publication. Similar studies should follow for other infrastructures.

Security Standards

The Commission considers the development of standards to be the responsibility of the infrastructure operators themselves. In our research, we were advised of an initiative of the NERC to apply mandatory reliability standards (which include security) to its members. Currently, the Federal Energy Regulatory Commission (FERC) is dealing with this issue for the whole electric power industry. The activities of these two organizations are headed in directions the Commission applauds and recommends to other infrastructure sectors.

However, we do believe that government should encourage and assist public and private sector standard-setting bodies to broaden their areas of responsibility regarding reliability to include security assurance.

We Recommend:	The National Institute of Standards and Technology (NIST) and NSA work with the proposed Office of National Infrastructure Assurance to offer their expertise and encourage owners and operators of the critical infrastructures to develop and adopt security-related standards. Relevant federal and state regulatory agencies, industry associations and standards groups, and law enforcement and intelligence agencies should also participate in the process of identifying and developing standards.[9] These standards should address not only the technology itself, but also ancillary topics such as tools, policies, procedures, and practices.

Building the Partnership State and Local Government

State and local governments are integral to the success of the partnership we propose for infrastructure assurance. State and local governments' infrastructure roles cut across the public-private boundaries. They operate infrastructures—certainly emergency services, but also water systems and a host of other vital services. They are also the regulators of many of the infrastructures—particularly those considered to be public utilities. And finally, they are users of the infrastructures—just as dependent on information and communications, energy, and transportation as the federal government.

We met dozens of local officials and held public meetings on infrastructures around the nation. State and local officials consistently expressed their need for federal assistance in key areas relating to infrastructure protection.

High on their agenda is raising public awareness on infrastructure matters, particularly in protecting information networks. They need assistance from the federal government in maintaining competent trained firefighters, policemen, and paramedics prepared to handle infrastructure disasters and threats from chemical, biological, and radiological materials. They need solutions

[9] Standard-setting groups include the American National Standards Institute, the Institute of Electrical and Electronic Engineers, and the National Computer Security Association.

in addressing the crowded spectrum of radio frequencies that emergency services must use to communicate. And they need a forum to share information on infrastructure issues.

Sharing Information

Organizations representing state and local interests have existing relationships with federal government officials. By working through such organizations, we can effectively share information on protecting our critical infrastructures.

We Recommend:	The proposed Office of National Infrastructure Assurance lead the way in making information about infrastructure assurance available to state and local governments through existing organizations such as the National Governors' Association.

Equipping and Training First Responders

The Commission's research found emergency services ill-prepared to deal with chemical and biological attacks. Few "first responders"—firefighters, police, and paramedics—are adequately trained to treat attack victims or equipped with protective gear or supplied with medical treatments, such as atropine.

Legislation initially sponsored by Senators Nunn (D-GA), Lugar (R-IN), and Domenici (R-NM) focused federal resources on providing training, equipment, and information to local first responders. State and local police, fire, and medical officials are requesting an expanded effort in this area, and the Commission agrees that these efforts should be intensified and made more widely available.

We Recommend:	DoD, the Department of Health and Human Services (HHS), and the FBI provide local first responders additional training and equipment for improving the detection, identification and management of chemical, biological, and radiological incidents. Domestic preparedness funding (Nunn-Lugar-Domenici) for these activities should be doubled in FY99.

Spectrum Allocation

Police, firefighters, paramedics, and repair crews must be able to communicate clearly during emergencies. The radio frequencies used for dispatching and communication are congested—making it difficult to use the spectrum effectively.

The FCC has been auctioning segments of the electromagnetic spectrum. As demand rises for commercial bandwidth, spectrum becomes increasingly scarce, placing non-revenue generating public sector users, such as federal, state and local emergency services, under increasing pressure to relinquish relatively under-used portions of their bandwidth allocations.

Addressing this issue, the National Telecommunications Information Administration (NTIA) and the FCC-sponsored Public Service Wireless Advisory Committee (PSWAC) issued a joint recommendation, which the Commission endorses, that the FCC designate inviolate spectrum segments for emergency services—removing them from future auction consideration.

Should circumstances require spectrum reallocation, however, the FCC should ensure compensation of state and local emergency service providers for the costs of replacement equipment, training, and transmission capabilities.

We Recommend:	Expanding NTIA's mission to include representing the interests of state and local governments in addressing access to and use of the electromagnetic spectrum. This advocacy should include efforts to ensure that current needs of these governments are identified and appropriately balanced with commercial and federal sector needs, that interoperability requirements among emergency services—in locales as well as regionally and nationally—are considered, and that adoption of new services and technologies is both facilitated and coordinated across all government levels.

We Recommend:	The FCC and NTIA expeditiously adopt the PSWAC recommendations. In particular, the FCC should: • allocate an additional 25 MHz of unencumbered spectrum for public safety. • provide 2.5 MHz in the VHF and UHF bands for interoperability among emergency service providers. • plan for allocation of an additional 70 MHz for new technology applications in law enforcement and emergency services. • immediately factor other detailed recommendations of the PSWAC into the spectrum allocation planning process.

These measures will assist state and local governments in meeting their critical infrastructure protection responsibilities, but they are only a first step. We fully recognize that the challenges facing state and local governments go well beyond what can be addressed by the application of such limited means.

Conclusion

In the interconnected, cyber-oriented world of today, the responsibility for infrastructure assurance cannot be divided along traditional lines between government and the private sector or allocated among levels of government. The need to forge a partnership between all players—to achieve joint, integrated, and complementary action—is more acute than ever. With a better understanding of the expectations and roles of the owners and operators, and of state and local governments, comes an appreciation for their increasingly "front line" mission in defending our infrastructures. The federal government should structure itself for its own mission of infrastructure assurance—a mission that now includes facilitating and supporting the efforts of critical infrastructure owners and operators.

(Intentionally Left Blank)

Chapter Seven

Structuring the Partnership

Objective

Establish national structures that will facilitate effective partnership between the federal government, state and local governments, and infrastructure owners and operators to accomplish national infrastructure assurance policy, planning and programs.

Early in the Commission's deliberations, we recognized the federal government was still organized along Cold War lines. The structures in place had proven very effective at focusing federal attention and resources on physical threats posed by military, terrorist, or criminal entities. Likewise, the relationships between government agencies and infrastructure operators were appropriate to the environment. Except for down-sizing, the structure of the federal government had not changed significantly since the Cold War, and its relationships with infrastructure owners and operators—though less regulatory in nature—had not changed markedly (see Figure 8).

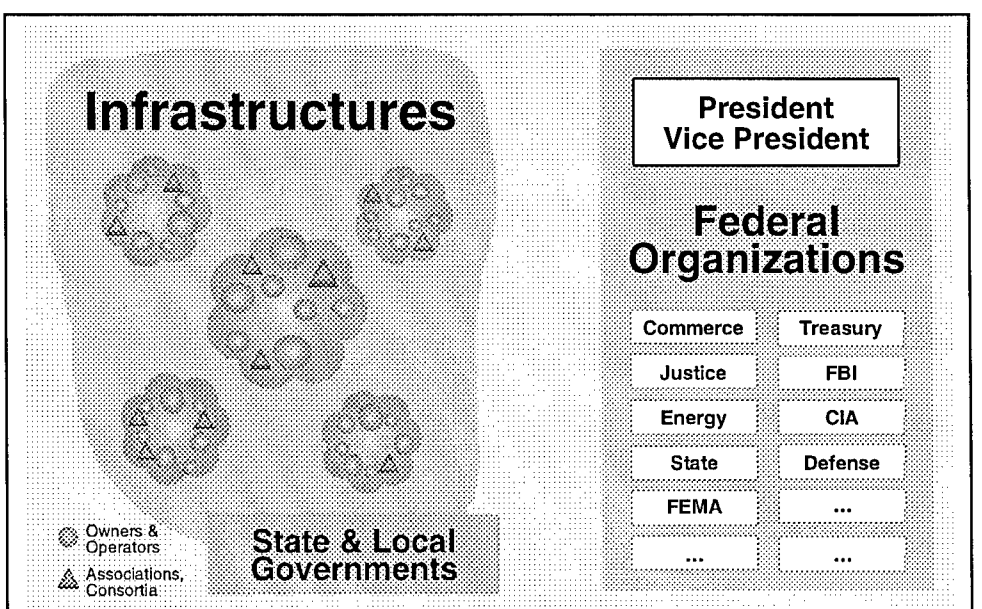


Figure 8. Infrastructure Assurance Today

But the federal government today must address the emerging threats to our infrastructures, the new geography discussed earlier in this report, and the requirements of the Information Age. How the government organizes itself is a key factor in the partnership with infrastructure owners and operators that is fundamental to meeting the

challenges of the threats we share. Without recommendations that set out clear national organizational structures, the chance for developing a government and industry partnership could elude our grasp.

To approach these organizational issues, we examined the functions or actions instrumental to achieving infrastructure assurance and protection at the national level. In each of the five functional areas, the need for partnership and dynamic interaction between the government and infrastructure owners and operators is apparent, as indicated below.

Policy Formulation—The federal government can best assess emerging threats, and the owners and operators can best assess their vulnerabilities. Together they should assess the national risk and determine assurance objectives, strategies, and policy.

Prevention and Mitigation—Owners and operators will have to examine the vulnerabilities of their own systems and networks and put in place the protective measures and practices needed to achieve target levels of assurance. The government can and should support these efforts through R&D, awareness and education, threat assessments, initiatives to facilitate private sector adoption of best practices, and , possibly, through direct financial assistance.

Information Sharing and Analysis—The key products of this functional area are answers to two questions: (1) What unusual is happening among our infrastructures, and (2) what unusual is happening among our adversaries? Owners and operators should take the lead for the former; the federal government (law enforcement and intelligence) for the latter. Analyzing the information provided and synthesizing it into advisories and warnings should be a shared responsibility.

Counteraction (incident management)—The objective of this functional area will be to deter and attack on our critical infrastructures, and, should deterrence fail, to cause the attacker to cease and desist. This area is clearly a federal responsibility, primarily of the law enforcement and defense communities, but there are many important ways in which the owners and operators can and should assist.

Response, Restoration, and Reconstitution (consequence management)—Responding to the basic needs of the populace following a disaster is a responsibility of the states, supported by the federal government. Restoring and reconstituting infrastructures is the responsibility of the owners and operators, supported by their sector. A major restoration and reconstitution effort would require coordinated public and private sector actions.

As we sought to identify what sorts of national structures would best accomplish these functions, we applied the same principles used to guide all of our deliberations.[10]

[10] These guiding principles are discussed in Chapter 4.

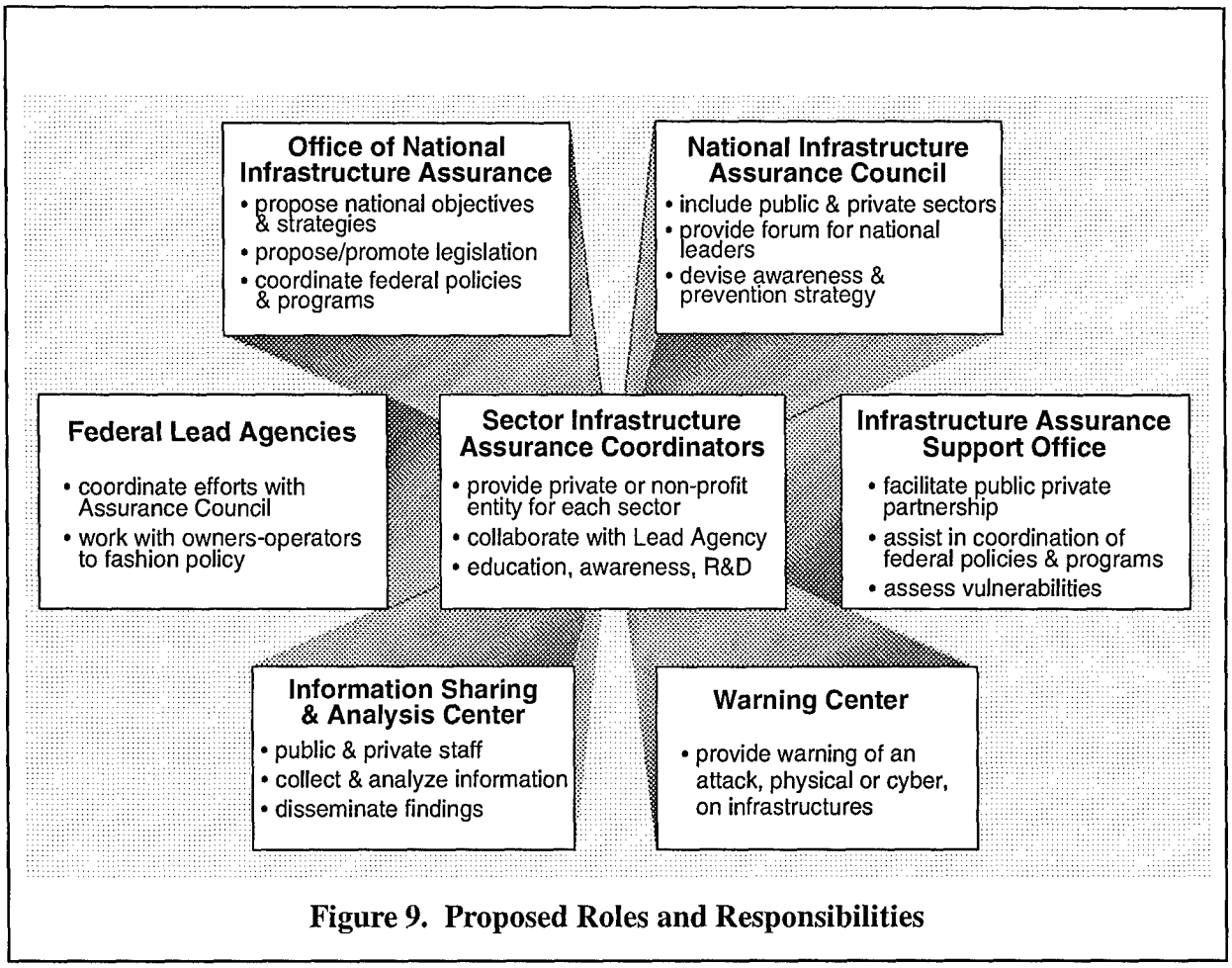


Figure 9. Proposed Roles and Responsibilities

Proposed National Structure for Infrastructure Assurance

The Commission proposes a set of structures and processes within the public and private sectors to facilitate infrastructure assurance functions and complement existing law enforcement, regulatory, and other channels of communication between and among critical infrastructure providers and the government. These new structures and processes will provide trusted and protected channels for sharing public and private infrastructure assurance information, and a means for focusing, enhancing, and generating additional infrastructure assurance efforts throughout the federal government and private sector.

Essentially, we envision the proposed infrastructure assurance structure for the United States as consisting of seven elements (see Figure 9). Each is discussed in detail below.

- An ***Office of National Infrastructure Assurance*** in the White House to serve as the focal point for infrastructure assurance.

- A ***National Infrastructure Assurance Council*** of prominent infrastructure corporate leaders, representatives of state and local government, and Cabinet officers to address infrastructure assurance policy issues and make appropriate recommendations to the President.

- An ***Infrastructure Assurance Support Office*** to provide functional support and management of the federal organizations involved in infrastructure assurance, as well as providing direct assistance to the public and private sector partnership effort.

- A federal ***Lead Agency*** for each sector to take the initiative in bringing together the owners and operators to create a means for sharing information that is acceptable to all.

- A ***Sector Infrastructure Assurance Coordinator*** for each infrastructure to function as a "clearing house," organizing information sharing activities, protecting the information provided by each participant, and acting as a channel for information to, and from, the government.

- An ***Information Sharing and Analysis Center*** consisting of government and industry representatives working together to receive information from all sources, analyze it to draw conclusions about what is happening within the infrastructures, and appropriately inform government and private sector users.

- A ***Warning Center*** designed to provide operational warning of a physical or cyber attack on the infrastructures.

No office, organization, or individual within the federal government has overall responsibility for infrastructure protection or policy. This is not surprising as there was little need for a national focal point when infrastructures were largely independent, discrete, insulated by geography and protected by military defenses. Today, however, the interdependent, interconnected nature of the infrastructures, and their exposure to cyber and other threats, creates a real need for a single point of focus. To support this, a federal framework needs to be created, working in conjunction with state and local governments and the private sector, to implement a national policy on infrastructure protection.

Our first recommendation for structuring the partnership between government and industry addresses this need for national focus by creating an Office of National Infrastructure Assurance.

Office of National Infrastructure Assurance ("National Office")

We Recommend:	The President establish a Office of National Infrastructure Assurance within the NSC staff, Executive Office of the President, directed by a Special Assistant to the President. The primary functions of the National Office would be government-wide policy formulation, oversight of government activities in infrastructure assurance and cyber security issues, and coordination of cyber support to existing and planned decision-making processes in the law enforcement, national security, counterterrorism, and intelligence areas.

The specific duties and functions of the National Office would include:

1) Oversee and facilitate infrastructure assurance policy formulation to include assessing the national risk, integrating public and private sector perspectives, proposing national objectives, developing implementation strategies, proposing and promoting new legislation, assessing the need for new regulations, providing oversight and functional management of infrastructure assurance budgets, and issuing national policy.

2) Encourage and support private sector prevention and mitigation activities including coordinating education programs, legislative and regulatory support to the establishment of standards, certifications and best practices, developing assessment instruments, and developing research requirements.

3) Oversee the creation, management, and operations of the other structures recommended in this report. The National Office would have special responsibility for oversight of the Information Sharing and Analysis Center, recommended below.

4) Review plans, sponsor appropriate training, and assess operational readiness. In the event the operational control of response to an attack on US infrastructures is elevated to the NSC, the staff of the National Office would serve as the secretariat to the NSC entity managing the crisis.

While this office would not have any operational responsibility for responding to an attack, we envision it as the channel through which federal cyber expertise and resources would be identified and made available to the decision-makers, planners, and the designated lead agency responding to an attack.

We envision this as a very small office, consistent with White House staffing standards. About ten senior personnel should be detailed from pertinent government agencies.

National Infrastructure Assurance Council ("Council")

We Recommend:	The President appoint a high-level council comprised of Chief Executive Officers (CEOs) from throughout the critical infrastructures, senior government officials (Cabinet rank), and representatives of state and local government. The Council would meet regularly to provide a forum for high-level discussion of proposed policies and directions for the nation in this critical area, to encourage and advocate partnership in infrastructure protection, and to make appropriate recommendations to the President.

The Council should provide policy advice to the President. It should meet no less than twice annually, and create whatever sub-structure it needs. A standing executive committee consisting of the Chair, selected Council members, and the Director of the National Office should meet often to manage the Council's work.

Staff support would be provided by the National Infrastructure Support Office. Members of the Council should be permitted to contribute staff and program support from their organizations (both public and private) to assist the Council in its work. Specific functions and duties of the Council should include:

1) Serve as the forum for national debate on infrastructure assurance issues.

2) Promote national objectives and strategies, facilitating discussion among the major stakeholders and government.

3) Review proposals from industry or government for mandatory standards, certifications, and best practices.

4) Provide leadership, advocacy, and support for the education and awareness efforts required to enhance national understanding and support for infrastructure assurance activities. Specifically, the Council should consider advocating, supporting, and encouraging adoption and use of "business" risk assessment tools and methodology.

5) Assist in setting directions for R&D program.

While the National Office and the Council provide avenues for the high level communication needed to develop a partnership in support of infrastructure assurance, the key to success in this arena rests with the existing federal agencies and the infrastructure sectors themselves.

Infrastructure Assurance Support Office ("Support Office")

We Recommend:	The President create a functional office to support infrastructure assurance activities throughout the federal government and the private sector.

The National Office would direct the activities of the Support Office, but it would be located in, and supported by the US Department of Commerce (DOC). The Support Office should be a joint coalition organization, bringing together appropriate national security and non-national security components. Staffing for the new office should reflect this mix among the required 20-30 professional, technical, and support staff including full-time employees, reimbursable details from other federal agencies, and private sector staff obtained under the Intergovernmental Personnel Act or by other means.

Its primary mission would be to support the National Office and the Council. Principal functions for the Support Office would include:

1) Support policy formulation by managing the national risk assessment, providing staff support to the Council and its subcommittees, tracking legislative and regulatory agendas, providing technical assistance to the Sector Infrastructure Assurance Coordinators, consolidating budget requests, drafting the budget proposal, establishing a system for tracking accomplishments, drafting the annual policy, and managing production and distribution.

2) Support prevention and mitigation by assisting the Council and the sectors in consolidating training requirements and developing new programs; by assessing current standards, certifications and best practices; by developing vulnerability assessment instruments (in consultation with the Sector Infrastructure Assurance Coordinators and selected owner and operators) and providing training in their use; and by coordinating the research program.

3) Assist the proposed National Office in the management of the Information Sharing and Analysis Center.

4) Assist the NSC in the preparation of stand-by plans and authorities in coordination with the relevant agencies and private sector entities; and provide technical support to the FBI and Federal Emergency Management Agency (FEMA) for development of policy and plans to manage incidents and consequences.

Federal Lead Agencies ("Lead Agencies")

We Recommend:	The President designate specific federal agencies to take the initiative in bringing together the owners and operators of various infrastructure sectors to create a means for sharing information that is acceptable to all participants. Lead Agencies will not replace the existing relationships, or assume any of the responsibilities of the law enforcement, regulatory or other special function agencies. They will work with sector owners and operators to identify and implement a method of sharing and protecting information.

Many federal and state agencies have interests and responsibilities in the infrastructure sectors. Additionally, each sector is comprised of diverse companies, associations and consortia which may challenge efforts to share information. Assigning leadership responsibility to the highest levels within identified federal agencies creates an opportunity to advocate and generate common purpose among the infrastructure leadership. We anticipate that Lead Agencies will coordinate with the Office of National Infrastructure Assurance to obtain the authorities needed to accomplish the following functions.

1) Establish and maintain channels of communication with all private and public entities having an infrastructure assurance interest in the sector.

2) Facilitate the selection of a Sector Infrastructure Assurance Coordinator (described below).

3) Assist the Sector Coordinator in establishing and operating an effective information sharing program.

4) Provide input to national infrastructure assurance objectives and strategies.

5) Draft new legislation and regulations, as required, and propose the use of federal incentives to facilitate private investment in assurance programs if appropriate.

6) Promote infrastructure assurance education and training, to include advocating use of best practices, within the sector.

7) Assist in developing plans for prevention (long-term reduction of vulnerabilities and short-term defensive actions), mitigation, restoration, and reconstitution.

8) Coordinate, in support of the Federal Response Plan (FRP), as amended, management of the consequences of a successful infrastructure attack and prepare for various contingent attacks through participation in training and exercise programs.

While assigning Lead Agency responsibilities for all critical infrastructures may be novel in some infrastructure areas, in others such a relationship already exists. Clearly, the Departments of Transportation and Energy already perform many of the responsibilities we outline for Lead Agencies. In other infrastructure sectors, telecommunications and information, for example, both DoD and DOC have significant interest and existing relationships in these infrastructure sectors. After much debate, we arrived at a proposal for assigning Lead Agency responsibilities for each infrastructure sector, shown in Table 2.

Table 2. Proposed Lead Agencies

Infrastructures from EO 13010	Commission's Infrastructure Sector	Proposed Lead
Telecommunications	Information & Communications	Joint Department of Defense & Department of Commerce
Electric Power	Electric Energy	Department of Energy
Gas & Oil	Gas/Oil Production & Storage	Department of Energy
Banking & Finance	Banking & Finance	Department of the Treasury
Transportation	All Sub-sectors	Department of Transportation
Water	Water Supply	Environmental Protection Agency
Emergency Services	Emergency Services	Federal Emergency Management Agency
Continuity of Government	Government Services	Office of National Infrastructure Assurance

Perhaps the most challenging responsibility of the proposed Lead Agencies will be facilitating the selection, by the owners and operators, of Sector Infrastructure Assurance Coordinators.

Sector Infrastructure Assurance Coordinators ("Sector Coordinators")

We Recommend:	Each infrastructure sector select or create an entity to facilitate sharing information among providers and with government. These Sector Coordinators will lead the sector in determining, collectively, how best to share the type of information needed for infrastructure protection by the federal government and owners and operators they represent.

Each sector will determine the particular mechanism best able to meet its needs. In some, an association or set of associations may best serve the industry and accomplish the role outlined here. Totally private and voluntary organizations may be selected by some, while others may find an existing regulatory agency more useful in the lead role.

Lead Agencies (described above) will work with infrastructure owners and operators and other government agencies that have industry-specific missions to establish these communication, coordination, and sharing mechanisms. Some sectors already have the kind of industry-wide organization needed. One example of such a partnership is the NERC.

Where a sector has such diverse interests that it cannot settle on a single Sector Coordinator, owners and operators and the Lead Agency may explore innovative solutions, such as a "virtual coordinator" based on existing networked resources.

The functions envisioned for the Sector Coordinators include:

1) Provide the sector with a means to accumulate information, disguise identity of providers, transmit information to the public-private Information Sharing and Analysis Center (described below), receive information from the Center, and disseminate it to the sector's owners and operators.

2) Serve as the focal point within the sector for risk assessment activities; and represent the owners and operators in discussions with other entities of the infrastructure assurance structures as needed.

3) Serve as the clearing house and hub for information sharing within the sector, assist in the analysis of anomalous events, and prepare statistical summaries.

Sector Coordinators will provide the central conduit for the information needed to develop an accurate understanding of what is going on throughout the nation's infrastructures. That is the purpose of the most innovative structure we recommend, a public-private analytic organization.

Information Sharing and Analysis Center ("Center")

We Recommend:	The President propose, and Congress charter, a new organization staffed by federal government employees and infrastructure owner-operator representatives to provide the analyses needed for infrastructure protection. The Center would receive information from all relevant sources, analyze it to determine what is actually happening in the infrastructures, and appropriately inform government and private sector users. Legislative changes will be required to implement this recommendation.

To be effective, the Center must have benefit of the legal initiatives discussed in Chapter 10, including some means to protect sensitive private sector information shared with the government and authority to negotiate non-disclosure agreements with the private sector. It should have direct channels to all interested government agencies to facilitate the flow of information.

Initially, the Center would focus on gathering strategic information about infrastructure threats, vulnerabilities, practices, and resources that will enable effective analyses to better understand the cyber dimension associated with infrastructures. The analysis produced will also allow more effective planning and decision-making about investments required within and outside the government. This information would include technical information of interest to owners and operators needing to better protect their systems from cyber attacks and threat-specific information developed by the government and provided through the Center to the infrastructure owners and operators. The Center would be expected to gather and maintain information about available assurance, protection, and defense resources within both public and private sectors for protection from cyber attack. Additionally, this Center would provide a one-stop/one-call capability for infrastructure assurance with special emphasis on the cyber dimension. When infrastructure owners and operators perceive problems within their information systems, they could call the Center to receive immediate information about available assistance.

The Center will, based on its analysis, issue bulletins, advisories, and other communications that will enable the infrastructure owners and operators to enhance their own levels of protection. It will also provide analysis to the FBI for dissemination to government agencies as required, and to the National Office and Support Office to be included in the policy, planning, R&D, budgeting, and other processes.

The responsibilities envisioned for this Center are:

1) Review reports of unusual occurrences from the owners and operators and the government, and prepare advisories for open release to the infrastructure providers through their Sector Coordinators and the government concerning vulnerabilities, failures, and system deficiencies.

2) Receive intelligence and law enforcement information concerning the development of potentially damaging tools and threats, and prepare advisories.

3) Enable the receipt and validation of anonymous data.

4) Provide technical assistance on a 24-hour basis.

5) Establish an extensive analytical data base accessible by the owners and operators and the government.

The proposed Center should eventually be staffed with between 20 and 40 personnel, about half of whom should be representatives from the infrastructures. Specific cost-sharing details can be negotiated, but to facilitate the speedy implementation of this recommendation, the government should be prepared to deploy the entire "start-up" cadre. The location of this Information Sharing and Analysis Center should be high on the agenda for decision by the Office of National Infrastructure Assurance. We believe an interagency group should investigate creative siting alternatives, especially locating it in the private sector. A number of excellent possibilities are available, among them co-locating with the Carnegie-Mellon University's CERT, another CERT, or a Federally Funded Research and Development Center, or contracting to a private entity (or university).

A significant aspect of the Center would be a government-only cell connected to the FBI's Office of Computer Investigations and Infrastructure Protection (OCIIP), which would serve as the preliminary national warning center for infrastructure attacks and provide the Center with law enforcement, intelligence, and other information needed to ensure the highest quality analysis possible.[11]

Information sharing and analysis will go far toward enabling the infrastructures to better protect themselves and ensuring the government has a more effective picture about what is happening throughout the infrastructures. This will allow us to understand whether diverse events—physical and cyber—are actually coincidental or related actions in an attack on different pieces of our infrastructures.

A Step Toward A National Cyber Warning Capability

We believe the eventual goal in this area is an indications and warning capability that provides immediate, real-time detection of an attempted cyber attack on critical infrastructures. The model for what we have in mind is the air defense and missile warning system. This is a defense system consisting of a monitoring or sensor capability, an analytic capability, and an alerting capability.

[11] In July 1996, the Director of the FBI established the Computer Investigations and Infrastructure Threat Assessment Center (CITAC) as a single point of coordination for all criminal, counterintelligence and counterterrorism computer intrusion matters and cases involving threats to critical infrastructures. In August 1997, the Director upgraded the status of this coordination function by creating the OCIIP.

Until we are able to field a real-time warning capability, we will need to rely on the proposed Information Sharing and Analysis Center described above and on existing government warning or watch centers. The FBI's newly-established OCIIP currently has the most potential for this effort and should assume the Warning Center responsibilities. In fact, the FBI has recently established and begun to staff a multi-agency Watch and Threat Analysis Unit within OCIIP. This unit's goal is to use existing criminal, counterintelligence, and counterterrrorism authorities to meld information from government sources and cooperating private sector entities to detect cyber threats to critical infrastructures. It will act on that information to provide tactical warning of immediate consequence. OCIIP will use existing mechanisms to issue cyber threat alerts in the same way the FBI now issues terrorist alerts. As new capabilities come on line in the Information Sharing and Analysis Center and with Sector Infrastructure Assurance Coordinators, we expect they will enhance the FBI's alerting mechanisms.

To integrate the capabilities being developed in OCIIP with those proposed elsewhere in this report, the Commission suggests that the OCIIP's function be expanded to include:

1) Operating near real-time secure communications with the proposed Information Sharing and Analysis Center on a 24-hour basis, in addition to the connectivity already being established by the Watch and Threat Analysis Unit with other government watch offices.

2) Integrating anomalous infrastructure events with intelligence and law enforcement information for the purpose of developing indicators that the nation may be "under attack." When such an indication is forthcoming, the FBI would make appropriate notifications and issue warnings, and would alert the Information Sharing and Analysis Center to prepare and disseminate bulletins and threat advisories to infrastructure stakeholders.

We consider development of a warning capability to be of fundamental importance to the future security of our nation. We urge the Director of the FBI to continue to enhance the capabilities of the OCIIP and we reinforce the FBI's requests for the funding needed to establish and maintain capabilities in the cyber arena—beyond those needed for the investigation of criminal, counterintelligence and counterterrorism cases—to include the analytic capacity and the R&D efforts related to threat detection that will enable real warning in the years ahead.

Tables 3 through 7 provide illustrations of how we believe these new structures would interact to accomplish the specific national functions required for infrastructure assurance. We mean them as a guide to the types of relationships, communications, and responsibilities that might develop as the recommendations of the Commission are being implemented.

Table 3. Policy Formulation	
Assess National Risk	Support Office lead, done by contract, reviewed by Council.
Integrate Public and Private Sector Perspectives	Council lead, consultation with sectors through Sector Coordinators; Lead Agencies and special function agencies support.
Propose National Objectives and Develop Strategies	Council lead, consultation with sectors through Sector Coordinators, Lead Agencies and special function agencies; proposed to the President through the National Office.
Propose and Promote (New) Legislation	Need identified by all sources, consolidated and analyzed by Support Office, validated by National Office, drafted by Lead Agency or special function agency, reviewed by Council and OMB, submitted to Congress.
Assess and Promote (New) Regulations	Need identified by all sources, consolidated and analyzed by Support Office, validated by National Office, drafted by federal or state regulator, reviewed by Council, reviewed by normal regulatory process.
Influence Private Sector Investments	Support Office with contract support identify deficiencies (based on emerging threats) either directly with Sector Coordinators or through the Council; Council recommends to companies through Sector Coordinators.
Prepare, Recommend and Promote Budget	Council, Lead Agencies, special function agencies indicate needs and make recommendations; National Office consolidates with Support Office assistance, package reviewed by Council, Lead Agencies, special function agencies, approved by National Office, submitted to the Office of Management and Budget (OMB).
Manage and Enforce Implementation	Results reviewed by Council.
Shape the International Environment	Subset of CSG/CT prepares, annually, international objectives, meet with Department of State to fashion strategy.
Issue the National Policy	Issued by the President with an endorsement from Chair of the Council.

Table 4. Prevention and Mitigation	
Provide Effective Education and Awareness	Threat analysis provided by Information Center and training requirements identified by Sector Coordinators; consolidated by Council; vendors identified and certified by Council; other education programs coordinated by Support Office; managed by appropriate agencies, such as National Science Foundation (NSF) and Department of Education.
Set Standards, Certifications and Best Practices	Established by Sector Coordinators; forwarded to Lead Agencies if legislation or regulation is desired by companies; Lead Agencies enter into legislative or regulatory process as required, if approved by Council.
Assess Vulnerabilities and Risks of System Components	Council directs Support Office to prepare assessment instrument for each sector requesting one; Sector Coordinators review instrument; assessment vendors identified and certified by Sector Coordinators; owners and operators fund and manage.
Research Advanced Techniques; Develop New Technologies	National Office determines requirements in coordination with Lead Agencies, Council, OSTP, and private sector research organizations; Lead Agencies and/or NSF request funding and manage research as agreed.
Negotiate Funding	Owners and operators identify system upgrades based on risk assessment; Sector Coordinators propose cost share; Council serves as the forum for negotiation with Lead Agencies and representative from National Office.
Acquire the Resources for Protecting Systems	Acquired by owners and operators.
Manage Operations Consistent with Best Practices	Managed by owners and operators; performance reviewed by Sector Coordinators supported by Lead Agencies.

Table 5. Information Sharing and Operational Warning	
Share Information	Owners and operators send information on "unusual events" to Lead Agencies, as required, and to Sector Coordinator information cells (connected to intelligence and law enforcement communities); threshold events and statistics to Information Center (also connected to intelligence and law enforcement).
Analyze Information and Prepare Threat Advisories	Information Center sends general advisories to all or selected participants as needed.
Disseminate Warnings	"Actionable" warning information is relayed by teleconference to the OCIIP for decision, with copy to National Office and CSG/CT duty officer; dissemination directly to Sector Coordinators and owners and operators as per protocol.

Table 6. Counteraction (Incident Management)	
Develop Incident Management Policy and Plan Operations	FBI develops incident management policy and plans; CSG/CT reviews plans; Sector Coordinators develop plans to "close holes and block attacks" using National Office threat information and planning guidance.
Deter, Halt, or Minimize an Attack;	NSC develops deterrence policy. FBI takes lead in any attack, assesses magnitude and requests assistance as required from Defense, Intelligence or other government agencies; lead may be elevated into NSC structure, supported by National Office secretariat.
Implement Defensive Actions	FBI notifies National Office and Sector Coordinators of nature and extent of attack concurrent with standard notifications; Sector Coordinators and FBI consult on recommended provider actions; Sector Coordinators notify owners and operators.
Punish Perpetrators During or After an Attack	FBI takes lead for response to both domestic and international perpetrators unless actions have significant diplomatic implications; in which case, lead is elevated to the NSC.
Control Misinformation and Manage Perceptions	White House stands up public affairs center assisted by law enforcement and intelligence communities, DoD, National Office, and others as needed.
Coordinate Incident and Consequence Management	FBI and FEMA negotiate directly, with National Office participation.

Table 7. Response, Restoration and Reconstitution (Consequence Management)	
Plan for the Response to Consequences	FEMA leads with support of Federal Response Plan agencies and state and local emergency managers.
Manage the Response to Consequences	FEMA leads with support of Federal Response Plan agencies and state and local emergency managers.
Plan for Restoration and Reconstitution	Owners and operators plan for routine disruptions; Sector Coordinators facilitate planning with support of Lead Agencies for major disruptions; planning consolidated by FEMA.
Manage Restoration and Reconstitution	Owners and operators manage routine disruptions; Sector Coordinators work through the Federal Response Plan using Lead Agencies for major disruptions; funding to be determined under provisions of the Stafford Act (PL 93-288, as amended).

Other Federal Responsibilities

Law Enforcement

The basic law enforcement functions are not changed. There is a relatively new class of computer crimes for which classical techniques and training may not be adequate. Federal law enforcement agencies lead the country in developing new capabilities and in conducting training and awareness sessions with state and local agencies.

Intelligence Collection and Analysis

The intelligence community is expected to continue and improve its programs designed to assess the likelihood of an attack from abroad in general and to give specific warning of increasing capabilities or specific hostile intent.

Emergency Planning

Because actions needed to save lives and protect property in the event of a major disruption of infrastructure services are much the same regardless of the cause, we expect that federal emergency planning and response functions will continue as currently constituted. The real key to minimizing losses, however, will be the rapid restoration of the disrupted infrastructures. While private industry has a commendable record of restoring operations after most conventional forms of disruption, in an orchestrated attack there is a potential for damage well in excess of that normally encountered. There may, therefore, be a need to develop plans and capabilities that do not now exist. In Chapter 10, we recommend that FEMA take action to consolidate restoration and reconstitution planning and operations under the auspices of the FRP, using the designated Lead Agencies.

National Defense

Certain threats to our infrastructures may rise to the level of a national defense concern. The magnitude of the threat and required response or the identity of the attacker (from beyond our borders) may shift the lead for a cyber attack from DOJ to DoD. DoD is expected to:

1) plan counteractions to deter, halt, or minimize an attack considering a variety of possible sources and alternative responses, which may include a variety of military options;
2) coordinate selection of specific responses with the National Command Authority; and
3) execute counter-actions as authorized.

In addition, as technology enables increased detection and identification capability for cyber attacks, DoD (including its NSA component) may play an increased role in detecting potential cyber attacks before they enter the nation's domestic communications systems.

International Outreach

In the new geography, protecting our infrastructures at home is not enough. Many aspects of infrastructure operations extend beyond our national borders, and even beyond the control of

their owners and operators. The very nature of the cyber dimension renders national borders almost obsolete, and national laws and policies based on those borders of less and less consequence. Initiatives to construct partnerships between and among sectors and infrastructures must of necessity take into account the international character of business. The overall success of our own infrastructure assurance efforts will therefore require substantial international collaboration. The federal government should continue efforts to work with appropriate international bodies to address infrastructure protection concerns and raise the level of international cooperation and coordination on computer intrusion matters. An effective international regime to deter cyber crimes and cyber attacks will be more effective than purely national sanctions. Clarification of the dynamics surrounding a "cyber attack" under international law would also contribute to deterrence. Other issues worthy of international dialogue include the handling of cyber crimes that transcend borders, and legal responsibilities in multi-national infrastructures. Diplomatic efforts can also contribute to the success of our national encryption policy and the development of internationally accepted standards for computer security and information technology.

The United States is not alone in facing the realities of the new geography, but we are definitely in the vanguard of countries which have begun to realize the urgency of the issue. This gives us an opportunity to shape the contours of international cooperation in this universally important area. Just as the federal government can lead by example in the context of US infrastructure assurance, the US can help create a positive influence on the infrastructure owners and operators—as well as the governments—of the countries that reside with us in the global community.

Conclusion

Managing new risks in the Information Age requires a partnership between industry and government for many purposes, from policy making aimed at preventing a crisis through responding if such a crisis occurs. It also requires adding a cyber dimension to our existing capabilities. Our recommendations in this chapter seek to enable increased partnership with the private sector and, importantly, to increase capabilities within our existing structures (see Figure 10).

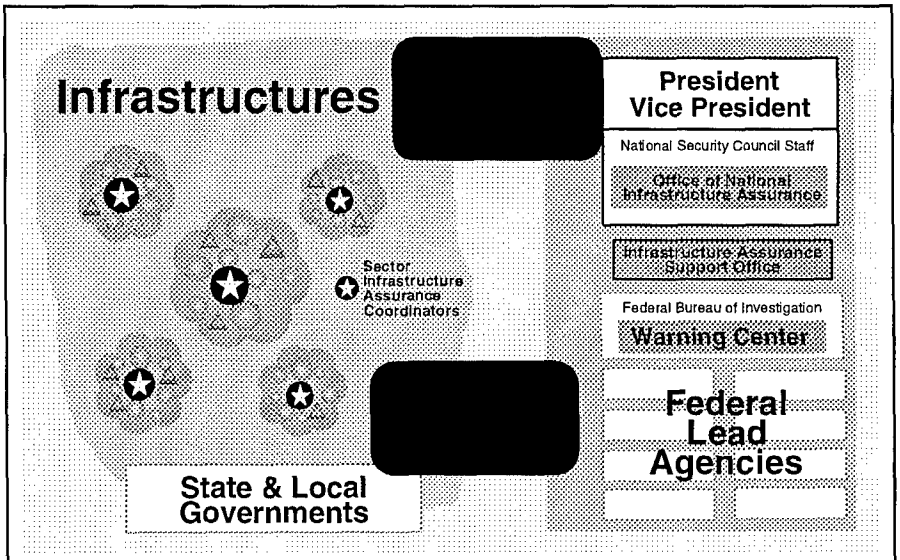


Figure 10. Proposed National Structure for Infrastructure Assurance

While we strongly endorse a policy of reliance on the private sector for problem-solving, solutions, and technology, we also see a need for a strong government focus on infrastructure protection and a federal framework to implement a national policy on infrastructure protection.

The key to success of the integrated public-private structure we propose will be "buy-in" from all sectors. And the key to their buy-in is heightened awareness of the challenges ahead. The new structures we propose are intended to generate awareness among all participants in infrastructure protection—public and private—and more broadly throughout the nation.

(Intentionally Left Blank)

Chapter Eight

Report on Awareness and Education

Objective **Elevate national awareness of infrastructure threat, vulnerability, and interdependency assurance issues through education and other appropriate programs.**

The Awareness Challenge

A successful public-private partnership requires a significant level of understanding on the part of the owners and operators of the infrastructures, government, and the public at large. It is clear that one key to a more secure future is broader understanding of the role that information and telecommunications play in our national security and economic competitiveness. That understanding must be supported by an increased knowledge base throughout the nation. We must have new "street smarts" about the Information Age, about computers, and about the communications systems that connect our institutions, homes, and businesses. In short, we need a new awareness throughout the nation.

The National Research Council cited the need for greater sensitivity to information security in a 1991 report:

> *"That today's commercial (computer and software) systems provide only limited safeguards reflects limited awareness among developers, managers, and the general population of the threats, vulnerabilities, and possible safeguards. Most consumers have no real-world understanding of these concepts and cannot choose products wisely or make sound decisions about how to use them. Even when consumers do try to protect their own systems, they may be connected via networks to others with weaker safeguards — like a polluting factory in a densely populated area, one person's laxness in managing a computer system can affect many."*[12]

[12] Computers at Risk: Safe Computing in the Information Age, National Research Council, National Academy Press, Washington, DC, 1991, pp. 2-3.

There are indications that awareness of computer security issues may be increasing, as demonstrated by a recent survey of 10,000 subscribers conducted by *Info-Security News* and Deloitte & Touche. Of the 1,225 responses, 55 percent considered lack of end-user awareness to be a significant barrier to information security. This is an improvement over the 73 percent who provided a similar response two years before, but it still suggests a requirement for greater awareness of the need for special measures to ensure information security.[13]

An Awareness Program

We have some experience with awareness programs. Forty years ago, wild fires annually destroyed nearly five million acres of land in the United States. Often caused by careless hikers, these fires cost nearly $1 billion per year. The "Smokey Bear" campaign, with its "Only you can prevent forest fires" slogan, saved about $17 billion in its first 30 years.

In the infrastructure protection arena, we need to reach four target audiences: infrastructure owners and operators, corporate infrastructure users, senior governmental officials at the federal and state levels, and the general public.

We Recommend:	The White House sponsor a series of conferences with national leaders in the public and private sectors to define programs to increase the commitment to information security. White House leadership is essential to the success of an awareness program on information security.

We Recommend:	The intelligence and law enforcement communities and the proposed Office of National Infrastructure Assurance expand existing programs of communication with infrastructure owners and operators and senior governmental officials by including periodic briefings on threats and vulnerabilities, recognizing the need to comply with appropriate security considerations.

We Recommend:	The National Academy of Sciences and the National Academy of Engineering establish a Round Table bringing together federal, state, and local officials with industry and academic leaders to develop national strategies for enhancing infrastructure security and to provide continuing support to an awareness program.

[13] Info-Security News Industry Survey, May 1997, pp. 20 ff.

We Recommend:	The proposed Office of National Infrastructure Assurance, in coordination with the private sector, spearhead a continuing national awareness campaign, emphasizing infrastructure security.

We Recommend:	The proposed Office of National Infrastructure Assurance establish a program to hold infrastructure assurance simulations involving senior public and private officials. Funded from the proposed R&D budget, the simulations would assess the value of new concepts in improving infrastructure assurance. Reports on the findings of the games would be distributed as a part of the awareness campaign.

We Recommend:	The proposed Office of National Infrastructure Assurance encourage the private sector to develop generally accepted security principles to be used by internal and external audit institutions in their regular operational audit functions in order to sustain awareness in public and private institutions.

We Recommend:	The proposed Office of National Infrastructure Assurance encourage private industry to perform periodic, quantitative risk assessments of their information and telecommunications systems, to enhance awareness of new vulnerabilities. A quantitative risk assessment addresses risk and likelihood of loss in business language and supports cost-benefit analysis for financial risk management.

An Education Program On Computer Ethics

In many families, children are more computer literate than their parents. Lacking experience, the parents seldom offer ethical guidance regarding computer usage. Universities are finding it necessary to establish new protocols for the student population in order to protect privacy and intellectual property. Computer ethics should be introduced as a field of study in all schools, from K-12 through universities.

We Recommend:	The White House convene a conference on the broad issue of computer ethics directed at the K-12 and the general university population, drawing on state and regional leaders who can support the programs in local communities, school systems, and universities.

We Recommend:	The US Department of Education commit at least $5 million per year for five years to assemble and distribute course materials and sponsor appropriate institutions for development of special programs and new course materials for K-12 and university education on the subject of the ethics of computer usage.

A Professional Education Program

There is a significant deficiency in the number of university faculty members equipped to teach information and computer security. Professor Spafford of Purdue University reports that "over the last five years, the four academic institutions teaching information security in computer science programs granted 16 Ph.D.s for security-related research. Of these, three stayed in academia."[14]

In schools of business, students majoring in information systems may learn about computer security. However, the students in other specialties who may become general managers are given little insight into the need to deal with information and communications security even in terms of their study of risk analysis.

The federal government has a number of initiatives under way in information security. DARPA has a research program that is helping in the design of security systems. NSA is developing a continuing workshop in this field. The second will be held in Austin, Texas, in 1998, organized by the University of Texas. These workshops are intended to share information about what is being taught in the field of information and communications security and how these educational programs can be extended to a larger audience.

We Recommend:	The White House convene one or more conferences of academic leaders from engineering, computer science, and business schools to review the status of undergraduate and graduate education in information security and identify changes in the curricula and the resources necessary to initiate needed changes to meet the national demand for professionals in the field.

[14] Statement of Dr. Eugene Spafford at "A Briefing on Secure Communications" before the House Committee on Science, February 11, 1997.

We Recommend:	NSF commit $10 million per year for at least five years to university programs on information assurance to support graduate students and faculty in Departments of Computer Science or in Business Schools with a view toward increasing the quality of education, the number of graduates in information and computer security, and the number of faculty members teaching in the field. As a part of such support, authorize the acquisition of advanced equipment when essential to the academic purposes of the program.

A General Education Program

Deficiencies in the training of technicians are reflected in inadequate attention to computer security in day-to-day operations. Education and training are essential to developing the staffs necessary to manage and operate major information systems today. Technicians need a deeper understanding of the systems they manage than they are likely to get if they have only on-the-job training. The rate of growth of the knowledge base makes it necessary to provide for initial training and also refresher training at regular intervals.

There are many commercial institutions in the field of education and training as well as community colleges, university extension programs, professional society programs, and others. While some have good course material, all could benefit from course material developed by the government agencies engaged in work in the field of information assurance.

We Recommend:	NIST, NSA, and the US Department of Education work in collaboration with the private sector to develop programs for education and training of information assurance specialists and for continuing education as technologies change. This effort should also support "training the trainers" to provide an adequate cadre of qualified instructors to teach technicians.

(Intentionally Left Blank)

Chapter Nine

Leading by Example

Objective **Initiate a series of information security management activities and related programs demonstrating government leadership.**

Infrastructure assurance is a joint responsibility, but the federal government has an unmistakable duty to lead the effort. Clearly, the federal government must ***lead by example*** as it reaches out to the private sector and other levels of government. We need to ensure the federal government has the policies and tools required to conduct business in the cyber age. Toward that end, the Commission makes these recommendations.

Improve Government Systems Security

The federal government has not paid sufficient attention to its own computer security needs. While OMB has developed and promulgated guidelines to ensure agencies adopt effective internal computer and network security practices, the effort to identify and replicate best practices throughout the government has fallen short of its target.

We Recommend:	Assigning systems security oversight responsibilities to the proposed Office of National Infrastructure Assurance. This will require legislative changes to restructure those responsibilities from OMB to the new office.

We Recommend:	The Secretary of Commerce and the Secretary of Defense charge NIST and NSA with assisting federal agencies in the implementation of best practices for information security within their individual areas. The process should include a NIST/NSA-facilitated assessment of agency vulnerabilities and security practices with input from the proposed Office of National Infrastructure Assurance.

We Recommend:	The FBI actively recruit college students with appropriate computer-related technical skills to seek employment with the Bureau. The FBI should consider offering part-time employment for skilled college students with regional computer crime squads. This program could produce current benefits as well as future special agent and forensic examiner applicants qualified to investigate cyber crime matters.

We Recommend:	The FBI facilitate hiring and retention of qualified personnel for technical analysis and investigation involving cyber attacks. Three years of service in cyber-related activities could be a condition of employment for those who receive a hiring preference based on computer skills.

Encryption

For electronic commerce to flourish, the information infrastructure must be secure and reliable. Protection of the information our critical infrastructures are increasingly dependent upon is in the national interest and essential to their evolution and full use. A secure information infrastructure requires the following:

- Secure and reliable telecommunications networks.
- Effective means for protecting the information systems attached to those networks.
- Effective means for authenticating communications of trading partners, assuring the integrity of data and non-repudiation of transactions.
- Effective means of protecting data against unauthorized use or disclosure.
- Well-trained users who understand how to protect their systems and data.

Strong encryption is an essential element for the security of the information on which critical infrastructures depend. Establishment of trustworthy key management infrastructures (KMIs) is the only way to enable encryption on a large scale, and must include the development of appropriate standards for interoperability on a global scale. Key recovery is needed to provide business access to data when encryption keys are lost or maliciously misplaced, and court-authorized law enforcement access to the plain text of criminal-related communications and data lawfully seized.

Neither private citizens nor businesses are likely to use the information infrastructure on a routine basis if they lack confidence that their communications and data are safe from modifica-

tion or unauthorized access. To ensure public confidence in key recovery, stored decryption keys must receive the same sort of legal protections that currently exist for mail, telephone communications, and electronic communications, including e-mail. To fairly balance the competing equities of privacy, electronic commerce, national security and law enforcement, and to ensure public confidence, the following are necessary:

- The public should be free to select an agent to issue digital signatures or to serve as a key recovery agent.
- Law enforcement agencies should have lawful access to the decrypted information when necessary to prevent or detect serious crime. Procedures for judicial review prior to granting government access must be defined in law.
- Individual rights of redress when access is abused should also be defined in law.

We Recommend:	Expediting the several government pilot projects underway or recently announced as a means of testing the technical and policy concepts involved and building public confidence and trust with the KMI key recovery approach. Further, the Administration should promote efforts to plan for the implementation of a KMI that supports lawful key recovery on an international basis. Finally, the federal government should encourage efforts by commercial vendors to develop key recovery concepts and techniques.

Procurement

We Recommend:	An interagency task force identify large pending procurements (such as the new Federal Telecommunications System, FTS 2000) related to infrastructure assurance issues, study whether infrastructure assurance objectives are being considered, determine how they may be adapted, and, based on the lessons learned, propose revisions to the overall procurement process.

Threat Assessments

We Recommend:	The federal government elevate and formalize information threats as a foreign intelligence priority.

NIST Risk Assessment

We Recommend:	NIST and appropriate government agencies continue development of risk assessment methodologies and make these known and available to the private sector, especially owners and operators of infrastructures.

Measuring Performance

The Government Performance and Results Act (GPRA) requires five-year strategic plans and performance measures for major functions and operations of federal agencies to be reviewed by OMB in the budget process. The Information Technology Management Reform Act (ITMRA) requires performance measures related to the use of information technology. The required performance measures do not, however, specifically include information security.

We Recommend:	The Administration direct federal agencies to include assigned infrastructure assurance functions within their GPRA strategic planning and performance measurement framework.

We Recommend:	The Administration and Congress amend the ITMRA to require that agency Chief Information Officers develop performance measures for the security of their information systems and to submit evaluations to OMB as required by the statute.

Certification Programs

The Environmental Protection Agency (EPA), NSA, and others have demonstrated ways of extending the benefits of federal standards or certifications to the private sector. The Commission noted the EPA's ENERGY STAR program as an example of such an effort. A recently-initiated certification partnership between NSA, NIST, and industry is designed to facilitate the evaluation of commercial information assurance products. These low cost, easily administered mechanisms encourage voluntary compliance with federal standards.

We Recommend:	Lead Agencies consider the creation and use of certification programs that are inexpensive to administer and enforce, and that provide incentives for adoption of standards for information security and information technology services and products.

Global Positioning System

The GPS is scheduled to be the sole source of radionavigation for aircraft landing guidance systems by the year 2010. Although cost-efficient, this creates the potential for single-point failure.

We Recommend:	The Secretary of Transportation: • Fully evaluate actual and potential sources of interference to, and vulnerabilities of, GPS before a final decision is reached to eliminate other radionavigation and aircraft landing guidance systems. • Sponsor an independent, integrated assessment of risks to civilian users of GPS-based systems, projected through the year 2010. • Base decisions regarding the proper federal navigation systems mix and the final architecture of the modernized NAS on the results of that assessment.

National Airspace System

The proposed architecture for the modernized NAS appears to have vulnerabilities that should be given full consideration before the final design is approved.

We Recommend:	The Federal Aviation Administration (FAA) act immediately to develop, establish, fund, and implement a comprehensive National Airspace System Security Program to protect the modernized NAS from information-based and other disruptions, intrusions and attack. Program implementation should be guided by the recommendations found in the *Vulnerability Assessment of the FAA National Airspace System Architecture*, prepared for the Commission.

(Intentionally Left Blank)

Chapter Ten

Legal Initiatives

Objective **Sponsor legislation to increase the effectiveness of federal infrastructure assurance and protection efforts.**

Infrastructure protection requires the integrated capabilities of diverse federal agencies, and special means for coordinating federal response to ensure that these capabilities are melded effectively together. The first step in defining federal structures to support infrastructure assurance in the Information Age must be to understand how responsibility is assigned today within the legal framework of the federal government.

The interdependence of all the infrastructures and the critical role of the information and communications infrastructure in all aspects of American life create special jurisdictional challenges. These jurisdictional problems are further complicated by the continued growth in cyber attack capabilities across the threat spectrum. The ability to know the origin, purpose and magnitude of an attack is significantly limited today. Consequently, we do not have the sharp and unambiguous jurisdictional cues that guide decisions about response and assignments of responsibility in the more familiar physical arena. We may not know the source of an attack—domestic or foreign. We may not know the identity or motives of the attacker—individual or group, terrorist, criminal, or government. Nor may we know the magnitude of the attack—whether a single system is involved or the attack is perpetuated throughout a network or series of networks. We may not even know if ours is the only nation experiencing the attack.

Given the lack of knowledge available at the initiation of an attack, it is clear that any required federal response will be borne on the Attorney General's authority as the nation's chief law enforcement officer. Elements of the response may require support of the defense, emergency response, intelligence and diplomatic agencies, as well as other agencies within government. There is a clear need to have required decision support, planning capabilities, and response authorities available to the Attorney General and to the White House should the decision reach that level.

The structures we recommend in Chapter 7 recognize that infrastructure assurance is more than a law enforcement, defense, or economic problem. It encompasses the responsibilities of each of

these areas, and also of the owners and operators who actually deliver infrastructure services. The federal government must not only integrate the familiar elements of government; it must also lead an effort to enhance the protection capabilities inherent in the infrastructures themselves, and generate the kind of trusted environment that enables a cohesive public-private partnership to accomplish all the functions involved in infrastructure protection.

We recognize also that while responsibilities are widely shared within the government, the current level of technology does not allow the posture of deterrence and forward defense that protects us from foreign military and terrorist threats in the physical dimension. Initially, all cyber attacks will have to be treated as crimes—regardless of where they originated or the purpose of the attack. When investigation provides evidence of foreign government involvement or the magnitude of the attack requires it, other leadership may be assigned. This also will require that the Attorney General have available immediate support from defense, intelligence and elsewhere in the government—especially from those agencies that have special skills and knowledge applicable to the cyber arena.

In making recommendations about increased partnership and better two-way sharing of information, we do not mean to indicate lack of support for existing efforts to build required information centers, watch centers, and command and control facilities. These efforts to enable response to cyber threats—criminal, terrorist or other—must continue. The organizations detailed in our recommendations are designed to expand the reach of existing capabilities, provide a means to coordinate and integrate them with information, knowledge and skills from the infrastructure owners and operators, and generally facilitate their efforts.

In addition to examining these jurisdictional issues, the Commission studied the legal foundations for infrastructure protection, and focused on the need to revisit the current law in light of infrastructure assurance objectives. In so doing, the Commission was able to make recommendations designed to enable the federal government to take a leading role, the private sector to respond, and the government and the private sector to engage in an effective partnership. Some of these recommendations, such as those relating to government model performance and legal impediments to information sharing, are highlighted in other parts of this report. Those recommendations as well as those contained in this chapter will provide a legal foundation for cultural change.

Enabling the Federal Government to Take the Lead

The first set of recommendations revisits existing legal frameworks for federal response to and deterrence of incidents involving the critical infrastructures.

Many areas of federal legislation that enable prevention and mitigation, response, recovery and reconstitution to incidents involving the critical infrastructures were written before the emergence of a recognizable cyber threat. It is not clear whether many of these authorities would apply, or should apply, to a major cyber-related event. Until the dynamics of such an event are better understood, major legislative change is premature. However, the Commission was able to identify key issues and make general recommendations to incorporate infrastructure assurance considerations within these legislative frameworks.

Defense Production Act

The Defense Production Act (DPA) provides authority to assist the reconstitution of critical infrastructures. The Commission reviewed DPA authorities, triggering mechanisms, and current modernization efforts for application to emerging threats, vulnerabilities, and related challenges.

We Recommend:	The Administration and Congress review the DPA in light of infrastructure assurance objectives. Specifically, we suggest: • Congress consider amending the DPA Declaration of Policy to include a finding that critical infrastructures are essential to national security. • Lead agencies associated with the critical infrastructures study the energy provision for priorities in contracts as a potential model for reconstituting other critical infrastructures. • Congress continue funding for the DPA Fund and financial incentives, and make funds available for R&D related to the critical infrastructures. • The Administration direct federal agencies with authorities pertaining to the critical infrastructures to review DPA authorities and work with industry to use these authorities when needed in response to a critical infrastructure incident.

Stafford Act/Federal Response Plan

The Stafford Act and FRP set parameters for federal response to major disasters as declared by the President. FEMA's authority to prepare for, mitigate, and respond to incidents affecting the operation of the critical infrastructures is unclear under the triggering mechanism currently contained in the statute.

Current FRP capabilities are responsive to infrastructure disruption. The capabilities and expertise to restore and reconstitute the infrastructures reside almost exclusively in the private sector and the main burden for planning and operations falls on the owners and operators of the infrastructure companies themselves.

However, the federal government has a shared responsibility to ensure that these infrastructures are restored rapidly in the event of a major disruption. The federal government should share in the costs of training and exercising, and ensure the availability of critical resources on a yet to be determined cost-sharing basis.

We Recommend:	The proposed Office of National Infrastructure Assurance study the Stafford Act, other authorities, and Federal Response Plan mechanisms for suitability in cyber-induced disasters. The study should address the potential impact of infrastructure failures and the desirability of direct assistance to infrastructure owners and operators.

We Recommend:	FEMA consolidate restoration and reconstitution planning and operations under the auspices of the Federal Response Plan, using the designated Lead Agencies.

Nunn-Lugar-Domenici

The Nunn-Lugar-Domenici legislation focused federal resources on providing training, access to equipment, and information to local first responders. State and local police, fire, and medical officials are requesting an expanded effort in this area. The Commission sees the need for more resources for training and equipment, and possibly an expanded scope to address other infrastructure-related events.

We Recommend:	Congress consider expanding the current Nunn-Lugar-Domenici program to incorporate other critical infrastructure issues, including attacks on infrastructures by means other than weapons of mass destruction, as well as training and information sharing efforts directed at state and local responders.

Adequacy of Criminal Law and Procedure for Infrastructure Assurance — Physical

In addition to the preventive aspects of the DPA, Stafford Act, and Nunn-Lugar-Domenici legislation, deterrence also plays an important preventive role against attacks on critical infrastructures. Deterrence through criminal law should be built not only through federal investigative and prosecutive capabilities, but also state, local, and international response.

Sentencing Guidelines

The Commission concluded there is adequate "legal fortification" from physical attacks. However, we identified several shortfalls relating to deterrence of crimes against critical infrastructures. The Sentencing Guidelines do not adequately address the severity of consequential damages arising from attacks on critical infrastructures—for example, damage resulting from the "downstream" effects of a denial-of-service attack. Consequently, a possibility exists of disproportionately light sentences for some forms of attack on critical infrastructures.

We Recommend:	The US Sentencing Commission expand the Guidelines to include greater flexibility to address actual and consequential damages, including "downstream" damage to property or loss of service resulting from attacks on critical infrastructures.

We Recommend:	The Sentencing Commission consider expanding coverage of its Guidelines to better address consequences of the use of biological and chemical weapons not resulting in death.

Interstate Commerce

The Commission identified two potential deficiencies with respect to purely intrastate attacks against critical infrastructures—even when attacks result in severe damage. In these instances, in order to assume jurisdiction over an investigation or prosecution, the federal government must demonstrate on a case-by-case basis that the incident affects interstate commerce. This is a difficult determination to make at the earliest stages of an investigation, before the scope of an attack is known or its effects are contained.

We Recommend:	Congress consider defining certain critical infrastructures as "instrumentalities of interstate commerce" to enable immediate investigation by federal law enforcement agencies and to subject those convicted to stiffer federal penalties.

Reward/Payment for Information Programs

The Commission reviewed legislation that offers rewards for information leading to the capture of terrorists. Under these legal authorities, Congress authorizes the Attorney General and the Secretary of State to administer rewards and payment-for-information programs. These laws effectively supplement other federal crime legislation to protect critical infrastructures.

We Recommend:	The monetary reward programs for information leading to capture and arrest of criminals be included as a line-item in participating federal agencies' budgets to ensure proper funding and implementation.

Adequacy of Criminal Law and Procedure for Infrastructure Assurance — Cyber

State & Local

Efforts are ongoing in most states to draft effective computer crime legislation. Dealing with juvenile computer crime is an area requiring greater attention. The states and federal government may be able to learn from innovative efforts in this area and consider modification to their laws to address what may be a growing problem.

We Recommend:	DOJ sponsor a comprehensive study aimed at compiling demographics of computer crime, comparing various state approaches to computer crime and discovering effective ways of deterring and responding to computer crime and abuse by juveniles.

Federal

The US Sentencing Commission's revised guidelines for the Computer Fraud and Abuse Act expanded definitions of "harm" and "loss" to include interruptions in service; disruptions or delays in delivery of vital services endangering lives; invasions of privacy; and the cost to the victim of damage assessment, restoration of service and data, and loss of business revenue due to interruption of service.

We Recommend:	The Sentencing Commission consider expanding its broader reformulation of harm and loss (in Guidelines Section 2B1.1, as it applies to violations of the Computer Fraud and Abuse Act and theft of trade secrets) to other forms of electronic crime and crimes relating to information and information technology.

DOJ is currently exploring ways to ease administrative burdens on federal law enforcement officers investigating various forms of computer and high technology crimes that cross federal jurisdictional boundaries. Of specific concern is allowing electronic searches to be conducted across jurisdictional boundaries with the authorization of only one federal judge.

We Recommend:	The Administration endorse and promote efforts currently underway to develop procedural changes to assist law enforcement in the investigation of computer crime, including modification of existing procedures for an effective nationwide trace and search warrant capability. Congress consider expeditious enactment of such legislation.

International

The US is a leader of efforts to clarify and improve current law enforcement procedures pertaining to computer crime.

We Recommend:	The Administration lead efforts to clarify and improve current procedures for investigating computer crime; work to create a network of international law enforcement agencies and telecommunications carriers to facilitate international investigations of computer crimes; and continue efforts to enhance international cooperation in computer crime investigations.

Legal Impediments to Vulnerability Assessments

Existing laws may create unnecessary legal impediments to the performance of vulnerability assessments on federal computer systems. The Computer Fraud and Abuse Act criminalizes a wide variety of misconduct premised on unauthorized access to government (and private) computer systems. The legislation is silent, however, as to how Red Teams might be *authorized* to attempt penetrations without running afoul of the criminal law. Legislative change does not appear to be required, but agencies should clarify procedures to facilitate sound vulnerability assessment practices.

We Recommend:	Federal agency Chief Information Officers establish procedures for obtaining expedient and valid authorization to allow vulnerability assessments to be performed on government computer systems. This requires a clear designation by agencies regarding who may authorize access to their computer systems for this purpose.

Enabling Private Sector Response

In addition to reviewing federal authorities that could be strengthened or expanded to allow the federal government to more adequately accomplish infrastructure assurance objectives, the Commission also considered potential legal impediments that might prevent owners and operators from taking appropriate action to safeguard portions of critical infrastructure within their control and responsibility. The recommendations contained in this section focus on providing owners and operators greater ability to take protective action.

Private Intrusion Response

Unauthorized intrusions often go undetected; when detected they may not be reported. Currently, computer security specialists and even state-licensed private investigators are gearing up to support private sector needs for computer security services. While their services fulfill some

victims' needs for confidentiality and control, potentially valuable information that could be used to assess the scope and nature of the threat is lost. Furthermore, there are no mechanisms in place to ensure the professionalism, qualifications, and methods by which these private investigations are performed.

We Recommend:	Congress consider new ways of facilitating the growth of private sector cyber-security capabilities that encourage increased sharing of information relevant to the scope and nature of the threat.

One approach to this area is nationwide licensing of private security specialists by a professional organization or the government. It might be possible to arrive at a professional licensing scheme that would provide benefits to a number of parties by specifying, for example, qualifications for obtaining a license, levels of insurance required, standards of practice, and conditions to allow for limited information sharing.

Additional prosecutive capabilities may also contribute to the current level of deterrence for computer-related violations. Prosecutive capabilities could be expanded by permitting victims the right to proceed in private civil actions. Civil remedies are currently available at federal and state levels. Improving the international availability of civil remedies is a logical extension of these efforts.

We Recommend:	The President seek to expand the availability of civil remedies for computer-related violations through appropriate multilateral and bilateral agreements.

Privacy Legislation and the Employer-Employee Relationship

"Insiders" provide the most frequent avenue of attack to the nation's critical infrastructures. The federal government guards against insiders' misdeeds through authority to conduct background investigations and periodic reinvestigations. Private employers who operate some of the critical infrastructures do not have the same ability. In many states, private employers do not have access to criminal history information; are prohibited from requesting or using criminal, financial or employment information; and may incur tort liability for revealing unfavorable employment history. These restrictions result from legitimate concerns over privacy, fair employment, rehabilitation, and related questions. We believe security considerations justify limited exemptions from these restrictions.

We Recommend:	The Attorney General convene a group of professionals from law, state and federal legislatures, labor and management organizations, and the privacy community to explore existing laws and recommend measures to balance employers' needs against individual interests in privacy.

We Recommend:	State legislatures consider adopting "consent" as a baseline for allowing employers to request background information from employees and potential employees for sensitive positions within critical infrastructures, subject to fair information practices.

We Recommend:	Congress narrowly expand existing exemptions to the Employee Polygraph Protection Act to include providers of information security services within the scope of its exemptions. This would update the legislation that currently allows polygraphs only to physical security services for certain public services.

Chapter Eleven

Research and Development

Objective

Increase investment in infrastructure assurance R&D from $250 million to $500 million in FY 99, with incremental increases in investment over a five-year period to $1 billion in FY 04. Target investment in specific areas with high potential to produce needed improvements in infrastructure assurance.

Federal R&D efforts are inadequate for the size of the R&D challenge presented by emerging cyber threats. Only about $250 million per year is being spent on federal infrastructure assurance-related R&D, of which 60 percent—$150 million—is dedicated to information security. There is very little research supporting a national cyber defense. The Commission believes that real-time detection, identification, and response tools are urgently needed. We concluded that market demand is currently insufficient to meet these needs.

R&D for infrastructure protection requires partnership among government, industry, and academia to ensure a successful and focused research and technology development effort.

We Recommend:	The President propose an increase in the federal investment in infrastructure assurance research to $500 million in FY99 and incremental increases in annual funding over a five-year period to $1 billion in FY04 for a targeted R&D program focusing on the six R&D areas listed below. • ***R&D Increases for Information Assurance.*** Assurance of vital information is increasingly a key component to the functioning of our interdependent infrastructures. The urgent need to develop new, affordable means of protection is apparent, given the increasing rate of incidents, the expanding list of known vulnerabilities, and the inadequate set of solutions available. • ***R&D Increases for Intrusion Monitoring and Detection.*** Reliable automated monitoring and detection systems, timely and effective information collection technologies, and efficient data reduction and analysis tools are needed to identify and characterize structured attacks against infrastructure.

	• ***R&D Increases for Vulnerability Assessment and Systems Analysis.*** Advanced methods and tools for vulnerability assessment and systems analysis are needed to identify critical nodes within infrastructures, examine interdependencies, and help understand the behavior of these complex systems. Modeling and simulation tools and test beds for studying infrastructure-related problems are essential for understanding the interdependent infrastructures. • ***R&D Increases for Risk Management Decision Support.*** Decision support system methodologies and tools are needed to help government and private sector decision-makers effectively prioritize the use of finite resources to reduce risk. • ***R&D Increases for Protection and Mitigation.*** Real-time system control, infrastructure hardening, and containment and isolation technologies are needed to protect infrastructure systems against the entire threat spectrum. • ***R&D Increases for Incident Response and Recovery.*** A wide range of new technologies and tools are needed for effective planning, response, and recovery from physical and cyber incidents that affect critical infrastructures.

We Recommend:	The National Research Council define, more fully, a national infrastructure assurance research program and lead an effort with departments and agencies already engaged in R&D relevant to each infrastructure.

Assuring Water Quality

Few infrastructures are taken for granted more than our fresh water systems. There is little chance of a threat reducing the quantity of available water sufficiently to endanger the population or cause industrial collapse. But there is risk of malicious attacks over time undermining public confidence. Alternatives for protecting the water supply are few. The most feasible approach we found is a research effort focused on water contamination detection technologies. Effective applications could be developed commercially and implemented at the state and local level.

We Recommend:	The creation of a specific R&D program to provide the scientific knowledge and technology necessary to allow highly toxic chemical and biological agents to be detected, identified, measured and treated in near real-time in the nation's water supply systems. The program should be administered by the EPA.

Provide Early Warning and Response

Real time detection of cyber threats is a special challenge to the R&D community. While this area is included in our recommendation above for additional R&D investment, it is central to the future security of our infrastructures. Some effort is under way, but it requires continued funding and high priority.

Although many industry and government groups are dedicated to ensuring the technical performance of next generation telecommunications networks, there has been no cohesive effort for protecting this infrastructure against the emerging threat of cyber attack. Such effort should include a system of surveillance, assessment, early warning, and response mechanisms to mitigate the potential for cyber threats. Although current methodology for this centralized effort does not exist, several of the basic technical elements required are successfully deployed on a small-scale basis, or in research, and could be integrated into a limited cohesive, national cyber response element.

Conceptually, a successful cyber attack warning and response system would include:

1) A means for near real-time monitoring of the telecommunications infrastructure.
2) The ability to recognize, collect, and profile system anomalies associated with attacks.
3) The capability to trace, re-route, and isolate electronic signals that are determined to be associated with an attack.

We Recommend:	The R&D program include a priority effort to develop such an Early Warning and Response capability.

Chemical and Biological Agent Detectors

Considering the serious and growing threat of a chemical or biological attack, chemical and biological agent detectors and effective protective and clean-up equipment are urgently needed and should be included in R&D efforts.

(Intentionally Left Blank)

Chapter Twelve

Implementation Strategy

This strategy provides the framework of objectives which will establish the foundations for a longer-term effort to assure our critical infrastructures. It describes major actions leading to fulfillment of each objective, and the expected outcome over the three-year period following a decision by the President to implement the Commission's recommendations. A more detailed implementation plan, with time lines, will be provided during the interagency review of the Commission's recommendations.

Strategic Objectives

Objective 1

Promote a partnership between government and infrastructure owners and operators beginning with increased sharing of information relating to infrastructure threats, vulnerabilities, and interdependencies.

Anticipated Three-Year Outcome

An active program which exchanges information on anomalous activities and suspicious incidents and distributes meaningful integrated analyses of government and private sector data, and threat and warning information, on an almost real-time basis to appropriate decision-makers in both government and private industry.

Action Items

- Develop a planning framework for establishing an Information Sharing and Analysis Center, jointly staffed by government employees and representatives from the critical infrastructures, to receive information from all relevant sources and conduct analyses for dissemination to participants.

- Designate selected federal departments and agencies to assume Lead Agency responsibilities.

- Coordinate with DOJ, other federal agencies, and the private sector to resolve legal impediments to information sharing, including potential antitrust, tort liability, national security, classification, disclosure, and protection of proprietary and trade secret information issues.

- Assist infrastructure stakeholder selection of Sector Infrastructure Assurance Coordinators to facilitate sharing of information among critical infrastructure owners and operators and with the government.

- Develop interagency infrastructure information sharing guidelines.

- Initiate personnel hiring process, identify an appropriate site, and stand up the Information Sharing and Analysis Center.

Objective 2

Ensure infrastructure owners and operators and state and local governments are sufficiently informed and supported to accomplish their infrastructure protection roles.

Anticipated Three-Year Outcome

Infrastructure owners and operators able to make better informed assurance investment decisions; local and state governments better equipped and trained to protect critical infrastructures and respond to untoward events.

Action Items

- Facilitate the efforts of NSA, DOE, and DoD to provide private sector assessments for critical infrastructure owners and operators; facilitate the offer of additional, more encompassing assessments over a range of cyber, physical, and interdependency risks; and provide vulnerability assessment training to private sector service providers on a cost-reimbursable basis.

- Encourage the private sector to develop generally accepted security principles to be used by internal and external audit institutions in their regular operational audit functions.

- Convene a group of professionals from law, state and federal legislatures, labor and management organizations, and the privacy community to examine existing laws in light of infrastructure assurance objectives and recommend measures to balance the legitimate needs of critical infrastructure owners and operators to conduct appropriate employee background investigations with the privacy rights of individual employees.

- Coordinate the continued development of risk assessment technologies, and associated tools, policies, procedures, and practices with appropriate federal agencies; encourage the transfer of these methodologies to the private sector; and encourage private sector performance of periodic quantitative risk assessments.

- Coordinate the development of mechanisms for disseminating information about infrastructure assurance to state and local governments.

- Encourage state legislatures to consider adopting "consent" as a baseline for allowing employers to request background information from employees and potential employees for sensitive positions within critical infrastructures, subject to fair information practices.

- Sponsor federal legislation to narrowly expand existing exemptions to the Employee Polygraph Protection Act to include providers of information security services within the scope of its exemptions.

Objective 3

Establish national structures that will facilitate effective partnership between the federal government, state and local governments, and infrastructure owners and operators to accomplish national infrastructure assurance policy, planning, and programs.

Anticipated Three-Year Outcome

A formal structure that encourages private industry participation in development of a national policy for infrastructure assurance, identifies the capabilities and responsibilities of federal agencies for infrastructure continuity, and facilitates national incident planning, response, mitigation, and restoration activities.

Action Items

- Establish an interagency working group to develop a plan for stand-up of structures that will contribute to the development of a national infrastructure assurance policy, including an Office of National Infrastructure Assurance; a National Infrastructure Assurance Council; an Infrastructure Assurance Support Office; and a Lead Agency to act as the government's focal point for each of the various infrastructure sectors.

- Review the FRP and other applicable documents to assist the FEMA's consolidation of restoration and reconstitution planning relating to cyber infrastructure assurance issues.

- Review results of legislative initiatives and other studies articulating roles and responsibilities of federal agencies for assurance issues; coordinate issues with appropriate entities.

- Coordinate a National Infrastructure Assurance Policy through government and private sector representatives.

Objective 4

Elevate national awareness of infrastructure threat, vulnerability, and interdependency assurance issues through education and other appropriate programs.

Anticipated Three-Year Outcome

A more informed private industry, government and general public who understand critical infrastructures; individuals and institutions who understand the need to protect their own use of information as well as information used by others; general appreciation of the need to develop a broader base of information assurance technical talent; and sharper focus on computer ethics and advanced information security technology in education programs.

Action Items

- Sponsor a series of White House conferences with academic and industry leaders from the public and private sectors to reach consensus on a plan of action that will increase the commitment to information security; emphasize computer ethics for grades K-12 and the general university population; review the status of undergraduate and graduate education relating to infrastructure protection, particularly information security; and define continuing opportunities to meet the national demand for professionals in the field.

- Coordinate with the National Academy of Sciences and the National Academy of Engineering to establish a Round Table in parallel with those in other fields, bringing together federal, state, and local officials with industry and academic leaders to develop national strategies for enhancing infrastructure assurance.

- Obtain NSF funding to support programs of professional education in university computer science departments and business schools.

- Coordinate with intelligence, law enforcement and regulatory agencies to expand programs for CEO briefings relating to infrastructure threats and vulnerabilities.

- Sponsor a feasibility study of publishing comparative infrastructure assurance-related data for certain infrastructures.

- Lead a public service campaign, in coordination with the private sector, to emphasize awareness of the threats and vulnerabilities of infrastructures and methods of improving infrastructure security.

Objective 5

Initiate a series of information security management activities and related programs demonstrating government leadership.

Anticipated Three-Year Outcome

Federal government information and networks are better protected from unauthorized intrusion, disruption, or modification using management procedures recognized as "best practices" and transferable to private industry.

Action Items

- Select a lead agency for assisting federal entities in the implementation of best practices for information security.
- Assign responsibilities for federal computer network security to the proposed Office of National Infrastructure Assurance.
- Encourage law enforcement to initiate new programs to hire and retain qualified personnel for investigative and analytical positions involving cyber issues.
- Fully evaluate threats and vulnerabilities associated with deployment of the GPS prior to elimination of other radionavigation and aircraft landing guidance systems.
- Develop, establish, fund, and implement a comprehensive security program to protect the modernized NAS from information-based and other disruptions, intrusions and attack.
- Resolve issues associated with spectrum allocation for communications among and between emergency service providers.
- Prepare an Executive Order requiring federal agencies to weigh the positive and negative effects on inrastructure assurance before publishing or requiring publication of information about critical components or functioning of infrastructures.
- Facilitate infrastructure assurance simulations within the federal government, and disseminate findings as part of the awareness campaign.

Objective 6

Sponsor legislation to increase the effectiveness of federal infrastructure assurance and protection efforts.

Anticipated Three-Year Outcome

Updated legislation that addresses critical infrastructure issues and enhances law enforcement ability to successfully investigate and prosecute related criminal activities.

Action Items

- Sponsor an interagency task force or other review mechanism to determine applicability of delineating infrastructure assurance objectives in the Information Technology procurement process; the Government Performance and Review Act; the Information Technology Management Reform Act; the Stafford Act; Nunn-Lugar-Domenici; and, the FRP.
- Formalize information threats as a foreign intelligence priority.
- Sponsor legislative activities leading to a finding that certain critical infrastructures are "instrumentalities of interstate commerce."
- Promote broader agency use of programs that provide monetary rewards for information relating to infrastructure attacks.
- Review information required by law to be published to ensure vulnerabilities are not disclosed.
- Coordinate DOJ sponsorship of a study to compile demographics of computer crime offenders, including juvenile offenders.
- Encourage the US Sentencing Commission to consider expanding its broader reformulation of harm and loss (in Guidelines Section 2B1.1, as it applies to violations of the Computer Fraud and Abuse Act and theft of trade secrets) to other forms of electronic crime and crimes relating to information and information technology.
- Endorse efforts currently underway to develop an effective nationwide trace and search warrant capability; and efforts to facilitate international cooperation in computer crime matters.
- Encourage the Sentencing Commission to expand guidelines to include greater flexibility to address actual and consequential damages, including "downstream" damage to property or loss of service resulting from attacks on critical infrastructures and, to better address consequences of the use of biological and chemical weapons not resulting in death.

Objective 7

Increase investment in infrastructure assurance research from $250 million to $500 million in FY99, with incremental increases in investment over a five-year period to $1 billion in FY04.

Target investment in specific areas with high potential to produce needed improvements in infrastructure assurance.

Anticipated Three Year Outcome

A focused and accelerated program which delivers usable tools to fill gaps in technology in infrastructure assurance.

Action Items

- Facilitate the establishment of a national focal point for infrastructure assurance R&D efforts and a public/private/academic sector partnership to foster technology advancement and transfer.

- Develop a comprehensive plan to focus R&D on technical solutions to infrastructure assurance issues associated with information security management, intrusion detection, vulnerability assessment and systems analysis, risk management and decision support, protection and mitigation, and incident response and recovery.

- Initiate an R&D program in cooperation with the water system owners and operators to identify vulnerabilities of water supply systems and to evaluate mitigation techniques.

(Intentionally Left Blank)

Onward

Originally, we had intended to title this final section of the report as a conclusion. It is anything but conclusion. In fact, it is a beginning. Our entire effort is prologue to a new era of infrastructure assurance.

This is not an exercise in problem solving. It is an attempt to deal with a rapidly changing, technology driven environment in which information and communications technologies add a new dimension of concern. In effect, we are not proposing solutions, but offering a step toward posturing our nation more effectively to deal with a new, still evolving world.

Our nation is in the midst of a tremendous cultural change, which will have a profound effect on our institutions. Accordingly, we are offering first steps toward preparing our critical infrastructures—and our government—to deal with this change. We believe that the only way to assure the future security of the nation is by assuring our critical infrastructures. And doing that will require a vigorous, innovative partnership between our government and the owners and operators of those infrastructures.

We offer these recommendations with a sense of urgency. While we do not believe a debilitating attack is imminent, the threats to our nation and the vulnerabilities in our infrastructures are real.

And the time to act is *now* . . .

(Intentionally Left Blank)

Appendix A

Sector Summary Reports

Executive Order 13010 designated as *critical* certain infrastructures whose incapacity or destruction would have a debilitating impact on our defense or economic security. Eight were named: telecommunications; electrical power; gas and oil storage and transportation; banking and finance; transportation; water supply; emergency services (including emergency medical services, police, fire and rescue); and government services. Because some of the eight listed infrastructures lent themselves to similar approaches, the Commission organized into five study teams to address the infrastructure sectors and industries listed below. This appendix provides summaries of the five sector studies, which will be published as separate appendices to the Commission's report.

Sector	Page
Information and Communications — The Public Telecommunications Network (PTN), the Internet, and millions of computers in home, commercial, academic, and government use.	A-2
Physical Distribution — The vast interconnected network of highways, rail lines, ports and inland waterways, pipelines, airports and airways, mass transit, trucking companies, and delivery services that facilitate the movement of goods and people.	A-11
Energy — The industries that produce and distribute electric power, oil, and natural gas.	A-24
Banking and Finance — Banks, non-bank financial service companies, payment systems, investment companies and mutual funds, and securities and commodities exchanges.	A-37
Vital Human Services — Water supply systems, emergency services (police,, fire, rescue, and emergency medical services) and government services (non-emergency services including Social Security payments, unemployment and disability compensation, and management of vital records).	A-44

Information and Communications

Introduction

The US information and communications infrastructure (I&C) sector generates more revenue than most nations produce. Far more than any other nation, the potential of the new technologies has enabled the US to reshape its governmental and commercial processes. We have led the world into the information age, and in so doing have become uniquely dependent on its technologies to keep our economy competitive, our government efficient, and our people safe.

Background

The I&C sector includes the Public Telecommunications Network (PTN), the Internet, and the many millions of computers for home, commercial, academic, and government use. The PTN includes the landline networks of the local and long distance carriers, the cellular networks, and satellite service. Switches automatically establish and disconnect circuits between communicating parties on demand. Prior to the introduction of cellular service in 1983, virtually all switched service was provided by the wireline telephone system. The system's two billion miles of fiber and copper cable remain the backbone of the I&C sector, with the newer cellular and satellite wireless technologies largely serving mobile users as extended gateways to the wireline network. The PTN provides both switched telephone and data services and long term leased point-to-point services.

The Internet is a global network of networks interconnected via routers which use a common set of protocols to provide communications among users. Internet communications are based on connectionless data transport. In other words, the Internet protocol does not establish a circuit between communicating parties during the lifetime of the communication. Instead, each message is divided into small packets of data. Routers forward the packets to other routers closer to their destinations based on address information in the packet headers. To maximize efficient use of the network, the routers may send each packet of a message over a different path to its destination, where the message is reassembled as the packets arrive.

The Internet and the PTN are not mutually exclusive, since significant portions of the Internet, especially its backbone and user access links, rely on PTN facilities. Current trends suggest that the PTN and the Internet will merge in the years ahead; by 2010 many of today's networks will likely be absorbed or replaced by a successor public telecommunications infrastructure capable of providing integrated voice, data, video, private line, and Internet-based services.

The installed base of computers in the US has risen from 5,000 in 1960 to an estimated 180 million today, with over 95 percent of these being personal computers. The remainder includes the majority of the world's supercomputers and roughly half of the world's minicomputers and workstations. Networking of these machines through the circuits of the PTN and the Internet has grown exponentially over the past 15 years, creating an extended information and communications infrastructure that has changed the way we work and live. This infrastructure has swiftly become essential to every aspect of the nation's business, including national and international commerce, civil government, and military operations.

Threats

The reliability and security of the I&C sector have become matters of critical importance. The primary threats to reliability are natural disasters and system failures. The primary threats to security are deliberate physical and computer, or "cyber," based attacks.

Because they are generally well understood, somewhat predictable, and geographically confined, natural disasters are the most manageable of the threats to I&C reliability. In recent large scale emergencies, telecommunications systems have proven highly resilient. The current policies and organizational arrangements for dealing with natural disasters are working and require no modification at this time.

A second threat to infrastructure reliability, less predictable and potentially farther reaching, is system failure arising from increases in the volume and complexity of interconnection and the introduction of new technologies. The unbundling of local networks mandated by the Telecommunications Act of 1996 has the potential to create millions of new interconnections without any significant increase in the size or redundancy of network plants. Unbundling will be implemented at a time of rapid and large scale change in network technologies. The interaction of complexity and new technologies will almost certainly expand the universe of ways in which system failure can occur, and, unlike natural disasters, there is no assurance that such failures will be localized. Nevertheless, demonstrated system performance, ongoing research, and the ability to modify legislative and technical timetables suggest that the challenge will be successfully managed.

While rapidly increasing complexity has characterized the I&C infrastructure since the breakup of the Bell System and the advent of the Internet, system reliability has remained extraordinarily high. Large scale system failures have occurred very infrequently and have been corrected within hours.

The Federal Communications Commission (FCC) and the telecommunications industry have actively researched reliability issues throughout the 1990s, laying the groundwork for the expected influx of new service providers and technology vendors. Major players in telecommunications have maintained a vested interest in network reliability and can be expected, as in the past, to collectively maintain and improve network performance. Finally, the legislative and technical imperatives underlying the restructuring and can be modified if serious difficulties

arise. The current framework of FCC regulation and industry standard setting are self-imposed and are expected to prove capable of accommodating the challenges to reliability posed by complexity and technological advance. This framework can be extended beyond its traditional switched network focus to cover cellular, satellite, cable, and the Internet.

The third and least predictable threat to the infrastructure comes from deliberate attack. Depending on their objectives, attackers may seek to steal, modify, or destroy data stored in information systems or moving over networks, or to degrade the operation of the systems and networks themselves, denying service to their users.

Attackers include national intelligence organizations, information warriors, terrorists, criminals, industrial competitors, hackers, and aggrieved or disloyal insiders. While insiders constitute the single largest known security threat to information and information systems, controlled testing indicates that large numbers of computer based attacks go undetected, and that the unknown component of the threat may exceed the known component by orders of magnitude.

Adversaries can employ a variety of methods against the infrastructure, including traffic analysis, cryptologic attacks, technical security attacks, physical attacks, and cyber attacks. Of these, physical and cyber attacks pose the greatest risk. They have increased rapidly in sophistication and disruptive potential during the 1990s, while the infrastructure's vulnerability has grown. The availability of truck bombs, chemical agents, and biological agents has markedly increased the disruptive potential of physical attacks. At the same time, the vulnerability of the I&C infrastructure to physical attack has increased as service providers have concentrated their operations in fewer facilities.

In the cyber dimension, tools to remotely access, change, or destroy information in vulnerable systems and to control, damage, or shut down the systems themselves have become more sophisticated, easier to use, and more widely available. Department of Defense tests and exercises, together with the rising incidence of documented intrusions and cyber-related losses over recent years, indicate that networked computers are highly vulnerable to these techniques. A broad array of adversaries, including a sizable number of foreign governments, are currently capable of conducting cyber attacks. The Defense Science Board expressed a mainstream view in its November 1996 estimate that limited strategic information warfare capabilities against the US infrastructure will to emerge over the next seven to ten years.

Vulnerabilities

The critical functionality of the PTN—increasingly software driven and remotely managed and maintained—is vulnerable to cyber attack. Deregulation will markedly expand the access points from which to launch an attacks. New entrants will be permitted to interface with the local exchange carrier networks at many different points, including local loops, switches, trunk lines, common channel signaling systems, advanced intelligent network systems, and operating systems. Technical details of the systems are widely available. Open interfaces and common

communications protocols will make intrusion easier by standardizing targets and simplify the propagation of attacks from one location in the network to other parts of the architecture.

The introduction of numerous third parties, including foreign companies operating in partnership with US companies or on their own, into every aspect of network operations will alter the trust relationship on which current network architecture is based. The security measures needed to compensate for the loss of trust will take years to develop. During this time, attacks to gain unauthorized access to sensitive data and functions will be easier to accomplish on a widespread basis than at any previous time in the history of telecommunications.

Switching

The susceptibility of the current generation of switching equipment to software based disruption was demonstrated in the collapse of AT&T's long distance service in January 1990. A line of incorrect code caused a cascading failure of 114 electronic switching systems. We believe AT&T's accidental failure could alternatively have been triggered maliciously by relatively small individual actions. Successor generation switching equipment now entering service is likewise potentially vulnerable to remote access, alteration, or control by skilled attackers.

Transport

Another major vulnerability in switched networks is the transport architecture. Transport refers to the transmission facilities used to move traffic between switching and hub offices within a network. Virtually all new fiber optic installations by commercial carriers are currently being configured as Synchronous Optical Networks (SONETs). Most of the elements in SONETs are managed remotely through packet data network connections vulnerable to electronic intrusion. In addition, SONET elements can be remotely attacked through maintenance and testing ports. The first large scale network outage known to be caused by cyber attack was the disruption of a "bulletproof" SONET ring.

Signaling

Common channel signaling (CCS) networks are connectionless data packet networks that carry instructions for call setup, special services, billing, and all other functions involving more than one element across the network. The potential for software-based disruption of common channel signaling was demonstrated in June 1991 when phone service in several cities, including 6.7 million lines in Washington, DC, was disrupted for several hours due to a problem with the network's Signaling System 7 protocol. The problem was ultimately traced to a single mistyped character in the protocol code. Current methods of protecting CCS networks from spurious messages are adequate to detect minor intrusions but are insufficient to protect the network from serious attacks. CCS network elements are also potentially vulnerable to tampering through remote access.

Control

Network operations are controlled by network elements that carry out tasks based on information received via signaling messages or retrieved from network databases. Traditionally, service control for voice telephone service resided in the switches. Implementing new services required

physical rewiring of the switching fabric. In recent years, local exchange carriers have been moving service logic to special purpose processing and database systems outside the switches, where it can be upgraded quickly through software changes alone. This control architecture, which permits rapid creation of custom services, is called the advanced intelligent network.

The ability of service logic programs to change the way the network reacts to subscribers' calls makes them a potential source of disruption if they are misprogrammed, corrupted by accident, or accessed and altered by adversaries. Access to service logic of all kinds is set to expand markedly as a 1993 FCC notice providing for access to the advanced intelligent network by third party service providers goes into effect. The FCC ruling states that these service providers must have the ability to incorporate their own service logic and add their own hardware to the network. As the network becomes more open, interfaces to third party providers will provide many new points of entry into the network and its signaling systems, increasing the potential for accidental or deliberate misuse.

Management

Management refers to the tasks associated with running networks on a day-to-day basis, including configuration management and maintenance. These tasks are for the most part automated and carried out from central locations using computer-based operations support systems. Today's high levels of automation and interconnection of network elements make manual management of the network virtually impossible.

Operations support systems are susceptible to a variety of attacks. An attacker can delay, replay, or alter the order in which messages are received, triggering unauthorized management operations. An attacker can alter the contents of management messages, tricking a network node into accepting management parameters that may affect the operations or configuration of the node, interfere with accounting, or disrupt traffic. An attacker can simply prevent exchanges between a managing node and its managed nodes, disrupting network operations.

In the coming years, as subscribers demand greater control over their network services, providers are expected to offer configuration management capabilities unprecedented in today's networks. Misuse of these more powerful capabilities will have the potential to disrupt or halt communications over significant portions of the network.

Network maintenance is increasingly performed through remote access. Remote access allows maintenance personnel to electronically access distant network elements to perform maintenance or management functions. Eliminating the need to physically dispatch repair personnel allows faster response to problems and more efficient use of maintenance staff. The channels used for remote access by authorized maintenance personnel offer potential attack routes for adversaries. Once logged on, an attacker can remove nodes from service and disrupt the network.

Operations support system capabilities have continued to increase in sophistication and in the number of network elements they can control simultaneously. The trend is to reduce the number of operations support systems in the network while expanding their ability to provide a multilevel view of network operations. This has led to the creation of megacenters, which concentrate op-

erations for large segments of the PTN and data communications networks in one location. A megacenter may service central offices extending over a multistate region, giving its operators access to every switch, operations system, and maintenance channel in the central offices served. An adversary with electronic access to a megacenter could target individual circuits, bring down selected services, or disrupt normal operations over large areas.

Another growing vulnerability in network management is the trend by public switched network service providers to manage network elements via the Internet. The Internet was originally built as a vehicle for information sharing in an open and cooperative environment. Security was not a primary design consideration. With its relatively uniform structure and uncomplicated protocols, the Internet offers less resistance than the public switched network to systematic attack. Its growing use in network management offers adversaries the opportunity to attack the PTN by disrupting the Internet. Improved security should be a key priority for the Next Generation Internet.

Findings

Today's level of threat and degree of vulnerability present two risks for national policy to address. The first is the cumulative risk generated by myriad small scale attempts to steal information or money through cyber attack. The vulnerability of individuals and enterprises to cyber theft damages the nation's current and future competitiveness. Losses undermine both the bottom line and public confidence in emerging information technology. For the information and communications infrastructure to realize its full potential as a medium for commerce, government, and military operations, users must have confidence that transactions will be confidential and protected.

The numerous security vulnerabilities in today's I&C infrastructure afford little basis for such confidence today, and the trends are not encouraging. In the meantime, the payoff for successful exploitation is increasing rapidly. With commerce growing exponentially over a medium with minimal protection, criminals and hackers can be expected to develop original and profitable new methods of operation. With larger and larger quantities of imperfectly protected information residing on networked systems, intelligence services and industrial competitors can be expected to find increasingly sophisticated ways to break in. To the extent they succeed, we lose competitiveness. To the extent we are forced to retrench in reaction to losses, we sacrifice opportunity.

The second and more critical risk is that presented by cyber and physical attacks intended to disrupt the US I&C infrastructure and the critical societal functions that depend upon it. With network elements increasingly interconnected and reliant on each other, cyber attacks simultaneously targeting multiple network functions would be highly difficult to defend against, particularly if combined with selected physical destruction of key facilities.

The possibility that such disruption could cascade across a substantial part of the PTN cannot be ruled out. Our experience with very large scale outages is extremely limited, and has dealt with reliability problems rather than deliberate and repeated attack. Network resilience has been as-

serted, but large scale testing is not feasible. Computer models capable of systematically analyzing security risks associated with large telecommunications networks have not been developed. No one knows how the network would react under coordinated attack. We do know that relatively minor software problems have produced cascading failures in the past. We cannot confidently set an upper limit on the disruptive potential of a planned, large scale campaign.

As the scale and objectives of potential cyber campaigns become more focused, their feasibility and potential for success increases. Achieving selected outages of regional targets, such as financial districts or ports of embarkation for deploying forces, is feasible for a greater number of adversaries than a major disruption of the national infrastructure, particularly if they have access to physical as well as cyber weaponry. Achieving outages of selected equipment, such as high density network elements serving large customer populations, is even more feasible. Noting the large scale outage achieved in a recent cyber attack on a SONET ring, widespread denial of service through remote attack is now a demonstrated capability.

To address the risk posed by the mounting incidence of cyber theft and other small scale attacks, national policy must encourage a cooperative approach to strengthening the security of the infrastructure. To address the risk posed by the vulnerability of the infrastructure to widespread disruption, national policy must ensure that there is an effective national capability to detect and defend against large scale attacks on the I&C infrastructure.

Recommendations

The US has led the world into the information age, and in so doing has become critically dependent on its technologies to conduct national and international commerce, governmental functions, and military operations. The protection of the US information and communications (I&C) infrastructure is a vital national interest.

Six years ago, the National Research Council's report *Computers at Risk* described the growing vulnerability of networked computers and outlined a series of core principles to improve security. Progress in implementing these principles has lagged, while vulnerability and threat have grown significantly. The vast expansion of computer networking, the increasing dependence of the PTN and the Internet on computer-based, remotely-managed control elements, and the increasing levels of interconnectivity and complexity mandated by the Telecommunications Act of 1996 have created new vulnerabilities to I&C reliability and security. Natural disasters, accidents, and system failures pose growing threats to infrastructure reliability, while increasingly powerful methods of physical and cyber attack pose growing threats to infrastructure security. With the I&C infrastructure having become vital to every critical economic, social, and military activity in the nation, effective action to implement effective assurance practices is a matter of great urgency.

Our I&C infrastructure encompasses a wide range of activities extending over vast reaches of physical and virtual space. No entity in government or industry directly controls more than a

small fraction of it. The problem of infrastructure security will require shared effort across organizational boundaries. No organization can solve it alone.

Implementing infrastructure protection policies is neither an entirely public nor an entirely private responsibility. The risks are common to government, business, and citizen alike. Reducing those risks will require coordinated effort within and between the private and public sectors. The need for infrastructure protection creates a zone of shared responsibility and cooperation for industry and government. If we are to retain and build upon the competitive edge information technology has given us, we need to work together to substantially improve the trustworthiness of our information systems and networks.

Strengthening Security Through Cooperation Between Industry and Government

To strengthen the security of the information and communications infrastructure, the Commission recommends that the federal government work in cooperation with industry to:

- Strengthen overall public awareness to gain acceptance of and demand for security in information systems.
- Promote the establishment and rapid deployment of generally accepted system security principles, beginning with those concerning password management and imported code execution.
- Promote industry development and implementation of a common incident reporting process.
- Increase accessibility of government threat and vulnerability information, expertise in system security assessment and product evaluation, and operational exercises to assist government and industry risk management decision making.
- Define and maintain metrics for security, along with the current set of reliability metrics, for public telecommunications networks.
- Actively promote network assurance research and development.
- Establish an international framework to support the use of strong cryptography on a global basis.
- Promote the development of effective security enabled commercial information technology and services. Accelerate the development and implementation of usable, affordable tools, methodologies, and practices in information security.
- Support uniform "one call" legislation against the "backhoe threat."

Defending Against Attack

An effective capability to defend the I&C infrastructure against attack in both the cyber and physical dimensions will require new sensing and warning capabilities, an organizational structure capable of dealing with the ambiguities of cyber attack, and new technologies for cyber defense. To ensure that there is an effective national capability to detect and defend against large scale attacks on the information and communications infrastructure, the Commission recommends that the federal government:

- Establish a focal point for national security policy on information infrastructure assurance and a focal point for national operational defense.
- Develop and sustain a robust intelligence collection, analysis, and reporting capability against cyber threats.
- Partner with private industry in developing and implementing indication and warning capabilities.
- Develop technologies needed for defending the nation's infrastructures against cyber attack, including after-action analysis and criminal investigations.

Leadership by Example

To serve as a national model for sound information assurance practices, the federal government should meet or exceed all applicable industry-based best security practices in building, operating, and using its portions of the information and communications infrastructure. Specifically, the Commission recommends that the federal government:

- Implement a common interdepartmental macro-level information systems security policy to standardize procedures and accountability.
- Require participation by all departments and agencies in annual information system vulnerability assessments, online security testing, and operational exercises.
- Establish clear visibility for information system security expenditures in the budgets of departments and agencies to facilitate management.
- Provide appropriate training and professional education in information assurance for all federal system managers, operators, and users, and assist state and local governments in establishing similar programs.

Physical Distribution

Introduction

The physical distribution infrastructure is critical to the national security, economic well being, global competitiveness, and quality of life in the US. The vast, interconnected network of highways, railroads, ports and inland waterways, pipelines, airports and airways facilitate the efficient movement of goods and people and provides this nation a distinct competitive advantage in the global economy.

Transportation is a major component of the US economy, representing in 1995 approximately $777 billion, or 11 percent of the Gross Domestic Product (GDP). US commerce depends heavily on the export, import, and domestic movement of raw materials, manufactured goods, foodstuffs, and consumable supplies.

The physical distribution infrastructure includes almost 4 million miles of public roads and highways and more than 360,000 interstate trucking companies, 20 million trucks used for business purposes, and 190 million personal vehicles. It includes more than a hundred thousand miles of track operated by the largest railroads, with 1.2 million operating freight cars and over 18,000 locomotives. It includes airlines that carry more than half a billion passengers a year through 400 airports. It includes almost 6,000 transit entities operating rapid transit rail and bus services. It includes 1,900 seaports and 1,700 inland river terminals on 11,000 miles of inland waterways carrying grain, chemicals, petroleum products, and import and export goods. The physical distribution infrastructure includes more than 1.4 million miles of oil and natural gas pipelines. And it includes delivery services, such as the US Postal Service and many other commercial providers that deliver goods and products on time not only to households, but to manufacturers whose very survival depends on just-in-time delivery of materials and supplies, and to business and even military activities who depend on the rapid delivery of repair parts to keep them in operation.

In this country, transportation is a matter of choice, and of intense competition. Commuters can choose between driving to work or taking mass transit. Travelers can choose to fly, catch a train or bus, or drive the highway. Shippers have their choice among highly competitive, customer focused delivery services and, in the deregulated world of transportation, among trucking firms, railroad companies, barge companies, and deep water shipping companies. Thousands of freight forwarders and consolidators, customs brokers and shipping agents move goods and cargo across the nation and through its ports quickly, cheaply, and effectively.

The US has the world's best transportation and distribution system, which both enables and reflects our having the number one economy in the world. Assuring that this system remains effective is critical to the well being of American citizens and the security of our nation.

Most of our nation's transportation infrastructure is owned by the private sector—railroads and pipelines; the vehicles and equipment operating on our roads, on the water, and in the air; and by state and local governments—our roads, airports, mass transit systems, and ports. The federal government owns the National Airspace System (NAS) operated by the Federal Aviation Administration (FAA), and the locks and dams operated by the US Army Corps of Engineers. The private sector is largely responsible for assuring its own infrastructure and business practices.

Trends

In the past, the business of transportation was conducted with paper—paper contracts and agreements, delivery orders, letters of credit, invoices, manifests, bills of lading, and shipping tags. Today, transportation, like other industries, is becoming increasingly enmeshed in our information-based society with its critical dependence on data and instantaneous communications.

While the transportation system has long been dependent on petroleum fuels, its dependency on other infrastructures continues to increase, for example, on electricity for a variety of essential operations and on telecommunications to facilitate operations, controls, and business transactions.

Demands on the physical distribution infrastructure continue to grow with the population and the economy. However, the ability to expand this infrastructure is limited. Rights of way for new roads, pipelines, railroads, and airports are difficult to obtain and justify. New means must be developed to make the existing system more efficient. Governments and industry have turned to information technology to increase that efficiency. Modernization of the NAS, extensive use and dependence on the Global Positioning System (GPS), and rapidly expanding use of Intelligent Transportation Systems (ITS) all will contribute to a more efficient transportation system.

Electronic commerce and data interchange, which make "just-in-time" delivery the norm rather than the exception, are increasing efficiency and giving companies a competitive edge in the global economy. However, requirements for open access to energy system data, increased dependency on data bases, and placing Supervisory Control And Data Acquisition (SCADA) systems on the public telecommunications network make these systems more vulnerable to unauthorized intrusion. The explosion of telecommunication requirements and intense competition in the communications infrastructure are leading to greater volumes of traffic on existing lines, thereby increasing the potential for "single point failures."

Railroad companies continue to merge, consolidating operations centers and lines, moving more and more traffic onto fewer corridors, and reducing the redundancy of the networks and increasing their vulnerability to physical attack.

Natural gas is being moved by existing pipelines without any agency or organization having a clear picture of the entire system or an understanding of its ability to handle surges in demand, or the tools necessary to evaluate the impact of a system-wide disruption.

The air traffic control system of the FAA is based on decades old technology. The replacement system, while doubtless more efficient, will be more vulnerable unless special security measures are incorporated.

Congestion is common in most metropolitan areas; ITS are being introduced to make more efficient use of existing road systems, but at the same time they will introduce new vulnerabilities. A discussion of the challenges specific to Emergency Services is provided later in this Appendix.

Public Expectations

The American public takes for granted freedom of choice among transportation modes and carriers, and generally wants government intervention limited to matters affecting safety and security. Transportation systems are expected to be reliable and predictable, designed and operated to allow unimpeded flow of goods through ports, across state and international boundaries, with rapid customs and immigration clearance processes and minimal regulatory and bureaucratic impediments.

Infrastructure maintenance and improvement must be adequate to ensure continued foreign investments in the nation's economy. A competitive level playing field within and between modes of transportation is crucial to freedom of choice and an efficient distribution system. Timely delivery of goods and products is essential, so we expect delivery services to be predictable and dependable. Government policies and regulations are expected to foster stability and consistency.

The public reluctantly accepts accidents involving planes, trains, and automobiles. But when the cause is found to be a failure of government oversight, such as substandard aircraft maintenance or a faulty traffic device, the public demands accountability. When a natural disaster affects the physical distribution infrastructure, the public expects rapid restoration. While the public anticipates and tolerates congestion on the nation's roads and highways, government is expected to use effective traffic management systems and techniques to minimize congestion. Gasoline, natural gas, and other energy supplies are expected to be available on demand.

Finally, the public expects a transportation infrastructure ready to respond to national crises, including adequate sea and airlift to move military forces quickly to any trouble spot on the globe.

Federal Role

The US Department of Transportation (DOT) provides national policy, funding, and safety requirements through its operating agencies:

- Office of the Secretary of Transportation (OST)

- Federal Aviation Administration (FAA)
- Federal Highway Administration (FHWA)
- Federal Transit Administration (FTA)
- Federal Railroad Administration (FRA)
- US Coast Guard (USCG)
- Maritime Administration (MARAD)
- Research and Special Programs Administration (RSPA)

DOT works to maintain the integrity of the US transportation infrastructure against terrorist and other criminal acts through a combination of regulations, guidelines, inspections, cooperative agreements, and government investments. Intermodal and interagency intelligence matters and security related actions are coordinated by and with the Office of Intelligence and Security within OST. Security actions are carried out by the DOT operating agencies, commensurate with their respective authorities.

The FAA, Coast Guard, and, to a limited extent, RSPA's Office of Pipeline Safety, are the only DOT agencies with clear statutory authority related to security.

Civil aviation security remains DOT's first priority and primary focus. The FAA has the responsibility and the authority to require contingency measures for air carriers and airports to deal quickly and effectively with immediate threats against civil aviation.

The Coast Guard has authority to respond to threats against cruise vessels and ports in the US and against vessels anywhere in the world carrying US citizens. The Coast Guard can institute regulations to establish and manage security zones around important facilities or operations, and to require certain port facilities and cruise lines to implement security measures.

RSPA regulates the design, construction, testing, operation, and maintenance of natural gas and hazardous liquid pipelines and liquefied natural gas (LNG) facilities; specific security authority exists only for LNG facilities.

Security authority and contingency plans for land transportation, including mass transit, railroads and highways, tunnels and bridges, and for a major portion of the nation's pipeline system, do not exist within DOT. Millions of people use passenger rail daily, and as shown by the 1995 Aum Shinrikyo gas attack in Tokyo and bombings of the subway system in Paris, mass transit remains open and vulnerable to terrorist acts. Millions of miles of pipelines carry natural gas and other hazardous materials throughout the country, and are largely unprotected and vulnerable to sabotage. Railroads carry tons of hazardous materials through heavily populated areas with little consideration given to the possible impact of intentional attack. Despite the possible national level political implications of a terrorist attack, protection of railroad, highway, and mass transit facilities remains the responsibility of industry or state and local governments.

Threats and Vulnerabilities

Transportation is inherently vulnerable to a wide range of physical threats. Natural disasters such as floods, earthquakes, landslides, and hurricanes are ever present; when these disasters strike, services are restored through the combined efforts of federal, state and local governments and the affected industry. As for man-made threats, with the exception of civil aviation, few countermeasures are available or appear to protect our transportation systems from physical attack by terrorists or other criminals. In the event of disruption from man-made causes, reconstitution and recovery are the responsibility of the owners and operators of the systems.

While the prospect of physical disruptions has been with the physical distribution infrastructure since its infancy, transportation industries are only beginning to focus on information-based threats or attacks. Many business systems are demonstrably vulnerable; this problem must be addressed by industry. To make intelligent decisions, however, industry leaders need current information on new and emerging threats. This information may be held within other companies in the same industry, in other industries, and within various agencies of the federal government.

Governments and industry have turned to information based systems to increase the efficiency of the public/private transportation system. While these increased efficiencies help keep our industries and companies competitive in the global economy, businesses are now much more vulnerable to electronic penetrations and attack and to disruptions of their supporting infrastructures, particularly telecommunications and electric power.

Conclusions and Findings

Today, information-based attacks cannot cause trains and planes to crash, nor are they likely to cause pipelines to rupture. Tomorrow—perhaps next year, perhaps in ten years—critical transportation systems could be vulnerable to such attacks and crippled unless action is taken now.

Roles, Missions, and Responsibilities

The Department of Transportation has been extremely proactive in counterterrorism efforts, both within the federal government and with the transportation industry. However, based on the Commission's outreach to industry and the federal government, several shortfalls in transportation infrastructure assurance, other than counterterrorism, have been identified:

- No defined roles, mission, and responsibilities for DOT in infrastructure assurance related areas other than counterterrorism.
- Lack of awareness and extremely limited availability of education programs.
- Incomplete or absence of vulnerability assessments of both physical and information-based portions of the transportation infrastructure.
- Limited and untested dissemination of threat information and warnings, and absence of an effective program to share critical information within the industry, and between the industry and the federal government.

- Absence of joint federal government/industry contingency or response plans to respond to an infrastructure threat or attack.
- Absence of security or assurance standards, guidelines, or best practices.

DOT is not well positioned to support the industry in infrastructure assurance efforts. The federal government must be involved with prevention, recovery, and reconstitution efforts within the transportation sector. DOT is neither funded nor staffed to address, with the industry, current or emerging threats to transportation.

Data Collection

Accounting for about 20 percent of all terrorist attacks around the world, transportation systems are a favorite target of terrorism. Better information and data on attacks would assist in development of countermeasures and provide better information for risk management decisions. Some modes of transportation are required to report all safety related incidents and accidents above a certain threshold, while others report through insurance agreements. These data are used to establish programs that can prevent and mitigate incidents and lead to cost effective improvements in safety. The private sector, however, is reluctant to report information-based attacks, fearing public disclosure of vulnerabilities that could be exploited by others and have a negative impact on public confidence in the industry. The physical distribution community is not an active partner in the improvements of data processing and communication systems, and as a result, has become more vulnerable with the extensive adoption of these systems.

Information Sharing and Threat Dissemination

Transportation is essential to the national economy and national security. Transportation is a high visibility terrorist target. Yet no agency or private sector organization is required to have, nor actually has, a program to advise the industry of information-based threats and attacks, nor are intrusions or attacks on the transportation infrastructure generally reported to the federal government.

No tested and effective means exists that facilitates reporting and transfer of information between the government and transportation infrastructure stakeholders on threats and attacks. Information-based threats to the physical distribution system are not addressed by DOT; private sector concern is on a sector-by-sector and company-by-company basis. Established reporting systems, where they do exist within the government and the transportation industry, are "stovepiped," and are not sufficiently shared or coordinated with DOT or with established national indications and warnings processes. Neither the federal government nor the private sector is tasked with identifying, quantifying and tracking information-based threats and attacks, nor is any organization responsible for analyzing and disseminating that data.

The apparent lack of information and sharing about information-based attacks on physical distribution systems limits industry understanding of the extent of the problem and makes it difficult to justify investment in measures to prevent or mitigate the impact of information-based attacks.

Industry representatives who receive information from DOT say they need more on the threat. The DOT is required by statute to notify the civil aviation industry of terrorist threats, but the statute does not require the DOT to notify the remainder of the transportation industry of threats.

Identification of Critical Assets

While industries are aware of critical assets within their companies, the federal government (e.g., DOT) has not identified and does not track those assets critical to the national security. Government/private sector contingency plans generally do not exist for responding to a terrorist threat or attack on the transportation infrastructure. While the transportation industry in general is capable of responding to natural disasters and other similar disruptions to their systems, coordinated plans to evaluate and/or respond to threats of a coordinated series of attacks on the transportation infrastructure have not been developed.

The transportation sector must be aware of and develop a process to protect key assets during heightened threat conditions.

- While the federal government is familiar with some of these assets, industry is in the best position to identify those facilities that require protection during national security events.
- Railroad, airline, highway, port and pipeline operation centers, among other facilities, are critical.
- A coordination process is essential to develop protection and recovery contingency plans.

The National Airspace System (NAS)

The present NAS is relatively immune from intrusions. It is composed of difficult-to-penetrate, dedicated subsystems, with the subsystems having different designs and older, specialized versions of software. However, the modernized NAS will undergo major new developments, including open systems architecture, and will depend on communications technology that permits wide interchanges of information among many of its subsystems.

The NAS would likely become a prime target for terrorism and "rogue" nation states during a national defense emergency.

Because the modernized NAS appears to be particularly at risk from information-based attacks; the FAA and Congress must take firm action to ensure adequate security measures are implemented with the new system.

1) The threat of attacks on the NAS subsystems has been low to date. There have been isolated incidents, including phantom controllers, during and immediately after the 1981 controller strike, and more recently at Roanoke, VA. While the FAA subsystems have not been subject to information warfare in the past, portions of the system still are vulnerable. For example, there have been recent instances of contractor use of FAA communications systems to access and modify software code under development and test.

2) Today's older NAS subsystems have some protective mechanisms built in to trap and remove damaged messages, unauthorized message types, and excessive flight plan filing activity. The subsystems also have many dedicated networks and different versions of proprietary software and communications protocols that make it difficult for intruders. But, their susceptibility will become more severe as the new NAS subsystems are installed.

3) During transition to the future NAS architecture, the level of vulnerability may increase as new systems elements are added to the NAS.

4) The nature of air traffic control operations provides a strong countermeasure that exists in real time within the NAS. Air traffic controllers are constantly observing the traffic under their jurisdiction and pilots are aware of unusual flight circumstances. This controller and pilot detection of system abnormalities will still be important in reducing the impact of any future attacks on the NAS subsystems.

5) The major vulnerabilities inherent in the new architecture are the planned use of new open systems and, using shared communications networks. Use of these new architectures, in conjunction with commercial off-the-shelf (COTS) hardware and software products, will increase the risk of insider and outsider (hacker) access, and the probability of malicious actions that interfere with the operation of NAS subsystems. These actions include data and software corruption, virus and Trojan horse damage. Use of shared networks will significantly increase the FAA system vulnerability to outside attack.

6) Systems with air-ground communications and data links such as the Automatic Dependent Surveillance-Broadcast mode (ADS-B), the Air-ground Data Link (ADL), and the Wide Area Augmentation System/Local Area Augmentation System (WAAS/LAAS) are susceptible to interference and signal jamming.

7) In the past there was a lack of priority and funding for establishing and conducting a security management program in the FAA, and for implementing information security protection for new automated and open system architectures. The situation is improving in that the top FAA managers forming the Joint Review Council (JRC) have recently identified a need for funding security provisions in the NAS, and have made a preliminary estimate of the funding levels to be included in future FAA budget submissions.

While the FAA has initiated the above effort to address security requirements for the NAS during its upgrade, the security improvements are currently unfunded and need Administration and Congressional support.

Pipelines

Two federal agencies perceive an assurance responsibility for the nation's pipeline system, presenting a unique situation as follows:

- DOT is statutorily responsible for regulating pipeline safety, and in some cases, for security.

- The Department of Energy (DOE) is statutorily responsible for oversight of the nation's energy supply; and as such has in place an effective intelligence and threat dissemination system.

These sometimes overlapping responsibilities must be clarified.

Regarding pipelines, current Environmental Protection Agency (EPA) efforts to publish "worst case scenario" data on the Internet raise serious concerns about the availability of targeting information for both terrorist and nation states. Access to this data should be controlled and made available to the public only on a limited basis. All federal agencies, not just DOT, and the industry, must consider the impact of making potential target information easily and readily available on the Internet and through other anonymous means; at a minimum, access must be controlled on a need-to-know basis.

Global Positioning System (GPS)

The Federal Radionavigation Plan calls for GPS and its augmentations to be this nation's sole radionavigation system by 2010. Current plans, if not modified, could lead to an over reliance on GPS based systems for critical transportation functions. The modernized NAS will depend on GPS and GPS augmentations as its sole navigation and landing systems. Exclusive reliance on any single system creates inherent vulnerabilities; no single system can be guaranteed for 100 percent availability for 100 percent of the time. Possible exclusive reliance on GPS and its augmentations, combined with other complex interdependencies, raises the potential for "single point failure" and "cascading effects."

Recommendations

Agency Roles, Missions and Responsibilities

The Commission is recommending that lead agencies be designated to promote the development of information sharing in respective sectors. Each designated lead agency would take a leadership and coordinating role with the private sector, and also seek appropriate legislation that allows for infrastructure assurance. The DOT, in assuming its responsibilities as sector lead for the Physical Distribution Infrastructure, should consider:

1) Establishing a central office responsible for coordinating intermodal infrastructure assurance as well as terrorism issues, including prevention, mitigation, contingency response, and recovery, and for coordinating with modal and other federal agencies, acting as primary contact points with industry on assurance issues.
2) Developing joint government/industry response and recovery plans with the private sector.
3) Establishing an improved information dissemination and sharing process.
4) Testing the effectiveness of the dissemination process and of established security procedures.

5) Working closer with industry on R&D and education.

6) Requesting for funding and positions to manage these emerging issues and responsibilities.

7) Reviewing of all proposed legislation for adherence with infrastructure assurance policies.

8) Obtaining appropriate executive and legislative authorities necessary to accomplish Lead Agency responsibilities.

Specific funding is necessary within OST and within individual DOT agencies for the following:

1) Providing government security clearances to industry, particularly for CEOs and CIOs.

2) Developing security and infrastructure assurance education programs.

3) Performing cross-cutting research on assurance issues, including GPS, the NAS, and train control systems, and for interagency research with agencies such as NASA and the Department of Defense (DoD).

4) Developing security standards or guidelines, and reporting systems.

5) Using secure telephones (STU III's), and encryption, strengthened firewalls, and other security measures.

6) "Red Teaming" and testing of critical DOT systems and industry systems on a co-operative, selective basis.

7) Conducting DOT sponsored industry symposia and workshops.

Education

Information security programs in the nation's business schools are very limited. Federal sector leads should promote and support development of undergraduate and graduate level programs and courses of instruction, including information security, with concentration in their specific sectors.

Pipelines

The Commission recommends the DOT and the DOE establish a formal process for addressing pipeline assurance issues in partnership with industry, clearly defining the responsibilities of each Department for security related processes, including threat dissemination, coordination, appropriate federal response to threats, possible establishment of threat levels, and developing plans for addressing potential and actual long-term, serious disruptions in the nation's energy supply.

Global Positioning System

The Commission recommends the Secretary of Transportation:

1) Fully evaluate actual and potential sources of interference to, and vulnerabilities of, GPS before a final decision is reached to eliminate all other radionavigation and aircraft landing guidance systems.

2) Sponsor a risk assessment for GPS-based systems used by the civilian sector, projected from now through the year 2010.

3) Base decisions regarding the proper federal navigation systems mix and the final architecture of the NAS on the results of that assessment.

The DOT and FAA must develop a better understanding of interference and other vulnerabilities of GPS before a final decision is reached concerning the status of all other radionavigation and landing guidance systems. A federally sponsored thorough, integrated risk assessment would lay a sound foundation for decisions on future courses of action.

The National Airspace System

The Commission recommends the FAA act immediately to develop, establish, fund, and implement a comprehensive National Airspace System Security Program to protect the modernized NAS from information-based and other disruptions, intrusions and attack. Program implementation should be guided by the recommendations found in the *Vulnerability Assessment of the NAS Architecture*, prepared for the Commission. The Vulnerability Assessment included the following recommendations:

General:

1) The FAA must clearly define responsibility for information security and accountability within its organization. The leadership should be able to make risk decisions that have budget and operational impacts. The FAA has established a NAS Information Security Group (NISG) to coordinate the information security activities of their many organizations, but the group does not yet have decision making authority on the information security (INFOSEC) that will be implemented in the NAS.

2) The FAA should enhance its security protection program with such traditional practices as: implementing and rigorously enforcing a highly visible security policy; planning countermeasures for known open system and COTS weakness; identifying and drawing from emerging infrastructure protection concepts; maintaining a Red Team for independent protection verification; providing an adequate level of electronic security staffing; and establishing a program for security education, training and awareness.

3) The FAA should consider the implementation of full "trusted" hardware and software security capabilities for only the FAA's most vulnerable future subsystems, since the software cost for embedded applications, together with full audit, tracking, and monitoring, may be too great if applied to all subsystems. Relaxation of the full capabilities, such as less rapid revalidation (e.g., a slower fifteen minutes down time) and less constant vigilance of data integrity, should be considered on a case-by-case basis for less critical subsystems, particularly in situations where existing air traffic control recovery procedures exist.

4) The FAA should conduct a comprehensive investment analysis of NAS INFOSEC in order to determine the degree of security protection that is needed.

5) The FAA should program funds for security provisions for the most critical subsystems in the range of two to four percent of subsystem cost, with additional funds as these subsystems become operational. The FAA should refine these percentage estimates and the identification of the subsystems they apply to, through a study of risk mitigation consequences, the degree of penetration testing needed, and INFOSEC life-cycle costs.

Automation: The FAA should provide virus protection, software distribution protection, and access control protection during the design, development, testing, and life cycle support of the future subsystems. Banner or warning screens should be used on all areas accessed by outsiders on computer and communications networks.

Communication:

1) Design the communications networks of the NAS in such a way that interconnections between the FAA administrative network and the NAS operational networks are kept to an absolute minimum and use well managed state-of-the-art protection methods including firewalls.
2) Monitor the use of Internet for backup communications, now in its preliminary planning stage, to avoid intrusions during systems outages.
3) Continue to use dedicated circuits for the most critical NAS assets.
4) Provide comprehensive security protection and maintain a physical separation between the Administrative Data Transmission Network (ADTN) and the Internet, and maintain a physical separation of this network from all critical operational subsystems. The current architectural plans call for multiple ties to the Internet. Computers used for administrative purposes at operational facilities should have no connection to any operational system.
5) Provide backup communications links and standby service contracts to support satellite communications links that fail or are jammed or flooded. The backup links should be capable of the automatic assumption of communications.
6) Ensure that Internet uses from computers that are connected to operational systems are avoided or have strict high-level approval and accountability for access to these systems.
7) Use encryption (never a complete solution for security requirements) on all critical communications links that have National Security implications (future and actual flight plans for Presidential aircraft, and key governmental and military officials).

Navigation and Landing:

1) Establish and maintain a backup navigation and landing system capability, possibly retaining elements of the current navigation and landing systems.
2) Provide full or partial backup for satellite uplinks for the WAAS system.

Surveillance: Provide surveillance backup for the ADS-B system, particularly in high density terminal areas, and in the center of the continental US, where primary radars are scheduled for removal.

Intelligent Transportation System

The Commission recommends that the DOT develop security standards or guidelines for ITS to assist agencies and companies in designing security into ITS systems during development and installation phases.

Crime

The Commission recommends that an intermodal forum, sponsored individually or jointly by industry or the DOT, be established to address the issue of criminal intrusion into unsecured shipping company databases and electronic data interchange, and the potential impact on critical business practices. The forum should be used to bring this issue to the attention of senior government officials and corporate management, assess the scope of the problem, and share best practices.

Anti-terrorism Legislation

The DOT has submitted legislation (H.R. 1720, the "Surface Transportation Safety Act of 1997") designed to protect the passengers and employees of railroad carriers and mass transportation systems and the movement of freight by railroad from terrorist attacks. The Commission recommends this legislation be given strong support from the Administration and Congress.

Energy

Introduction

The security, economic prosperity, and social well being of the US depend on a complex system of interdependent infrastructures. The lifeblood of these interdependent infrastructures is energy, the infrastructure composed of three distinct industries that produce and distribute electric power, oil, and natural gas. Profiles of these three industries are shown in Figures A-1, A-2, and A-3.

In addition to being a key component of the other infrastructures, the energy infrastructure is critical to our economy, with estimated revenues from retail sales of electricity in the US exceeding $200 billion annually, and revenues from oil and gas almost $400 billion. US energy consumption by fuel type is depicted in Figure A-4.

Today our energy infrastructure is the most reliable and robust in the world. While energy shortages and outages have made national and international news, they are rare. The handful of major incidents in modern times, dating back to the 1965 Northeast Blackout, includes the gasoline shortages of 1973 and 1979 and the electric power outages in the western US in 1996. Despite the proven reliability of the US energy infrastructure, however, there are significant challenges to sustaining this robustness and resilience in the near future.

Disparities in prices across the country are partially responsible for the recent restructuring of the electric power industry and natural gas industry (Figure A-5). New information systems for electronic commerce, for data interchange and for improving operational efficiencies are now essential business elements of the energy infrastructure. Electric utility and natural gas companies are merging and consolidating resources, while at the same time new transmission line rights-of-way are almost impossible to obtain because of the "not in my back yard" syndrome or environmental concern. With the advent of natural gas and electricity commodity markets, the number of marketing companies has grown exponentially, from eight in 1992 to more than 250 in 1996, while electric power capacity reserves continue to shrink. As in the telecommunications industry, the customer of the electric power industry faces a complex service industry in which no one company will provide end-to-end service.

The reliability of electricity has become more critical to our nation's competitiveness and standard of living in the Information Age. The use of natural gas to generate electricity is growing rapidly, as it is the current clean fuel of choice. And we are becoming ever more dependent on the supply of foreign oil, recently surpassing the 50 percent level for oil imports.

While the nation's dependence on less expensive foreign oil continues to grow, refineries in this country are being closed and, in light of thin profit margins and environmental constraints, no

new refineries are planned in the US. Over the last decade the oil industry has lost 450,000 US jobs to overseas operations, and one major company alone has reported a workforce reduction from 30,000 to 20,000 employees during the early 1990s. Some of these job losses are blamed on federal and state environmental regulations. To minimize costs and increase efficiency, many companies are dramatically expanding their automation and networking systems and are linking their control, administrative, and business information systems. Many companies are also consolidating their computer centers, with one major worldwide company consolidating its operations into a single megacenter.

Most physical threats to the energy infrastructure are well known and documented. As a result of concern about terrorists attacks, the National Security Council, Congress, the Department of Energy (DOE), and the energy industry focused on the physical security of the infrastructure during the 1980s. This activity led to public hearings by Senator John Glenn of Ohio in February, 1989, and was documented in the Office of Technology Assessment report "*Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage.*" In response to the government's concerns, the energy industries compiled internal lists of their critical assets and spare components. Processes were established to disseminate threat information, selected security personnel were cleared to receive classified information and forums were established to share information. As a step toward ensuring viability of energy infrastructures, DoD and the Federal Bureau of Investigation (FBI) initiated their Key Asset Protection Programs. Joint private sector and government exercises were conducted for mutual education and to test the emergency response capabilities.

As farsighted and laudable as these efforts were, however, interdependencies within the energy infrastructure and with the other infrastructures were not studied, nor was the energy sector's growing dependence on information systems. Without electric power other critical infrastructures, such as telecommunications and banking and finance cannot function. The transportation infrastructure would cease to operate as it relies almost exclusively on oil products. These linkages reflect the growing interdependencies between the infrastructures.

Some analysts postulate that the 1996 western power outage and the New England and MidWest summer power shortages were not isolated instances, but are indicators of an industry experiencing a weakening in its historically strong assurance program.

Threats

Threats to the US energy system arise from a number of sources including hostile governments, terrorist groups, other organized groups or individuals, disgruntled employees, malicious intruders, complexities, natural disasters, and accidents. More than a thousand reported incidents directed against the US energy system have been documented by the DOE over the last 15 years; some involved outages and significant damage. In recent years, cyber incidents, including deliberate as well as accidental malfunctions, have begun to appear.

Organized attacks on the energy infrastructures in other countries include an Irish Republican Army (IRA) plot to blow up energy and water installations and cause massive disruption across

London in the summer of 1996. A police raid in south London found 36 devices; the planned targets included six electrical substations, gas valves and pipelines, and water pumping stations. Six participants were found guilty of conspiracy and were sentenced to 35 years in prison. A more recent event occurred in Texas this April, when a group planted explosive devices on three natural gas holding tanks at a processing plant to divert police attention during a robbery attempt. It was believed the explosions would have released toxic fumes which could have wiped out half of the county.

The most common disrupter of energy supplies is inadvertent damage to buried cables or pipelines, such as is frequently caused by a "back hoe." However, these disruptions are usually localized and have no national level impacts.

Downsizing of the industries, partially in response to restructuring and consolidating pressures, leads to a significant loss of expertise that is difficult to replace. Downsizing also disrupts the traditional compact between employer and employee and creates a potential cadre of disgruntled "insiders." An estimate provided to the Commission by industry security directors was that 75 to 80 percent of the security incidents they experience are caused by persons from within the organization.

Managing consequences of natural disasters and accidents is an inherent part of the energy industries' operational processes. Their mitigation and response efforts and activities have high public visibility, and have resulted in an outstanding response by the industry.

Vulnerabilities

Specific areas of vulnerability addressed by the Commission's Energy team are categorized as:

- Electric Power: power generation (including fuel supply) systems, transmission systems, distribution systems, electric network control and protection systems.
- Oil and Natural Gas: supply, transportation, storage and distribution (pipelines are a joint effort with the Commission's Physical Distribution team).

The Commission's review focused on those elements of the infrastructure in which exploitation of a vulnerability could cause extended regional or national impacts. Nominal impact figures used were 500,000 people/customers affected for at least 12 hours.

Vulnerabilities facing the energy industries include:

- Those created in the operating environment by the rapid proliferation of industry-wide information systems based on open-system architectures, centralized operations, increased communications over public telecommunications networks and remote maintenance;
- Supervisory Control and Data Acquisition (SCADA) systems that are vulnerable because of use of commercial off-the-shelf (COTS) hardware and software, connections

to other company networks, and the reliance on dial-back modems that can be bypassed;

- Increased availability of vulnerability information, much of which is mandated by regulatory bodies to facilitate competition, and the tools for exploiting those vulnerabilities;
- Rapid assimilation of advanced technologies with their inherent complexities;
- Consolidation of infrastructure corridors (e.g., communication, electric transmission lines, pipelines, etc.); and
- Previously identified physical vulnerabilities of critical assets that have not been adequately addressed throughout the industry.

Electric Power Vulnerabilities

Of particular concern are the bulk power grid (consisting of generating stations, transmission lines with voltages of 100 kV or higher, plus 150 control centers and associated substations) and the distribution portion of those electric power systems whose interruption could lead to major metropolitan outages. (Note: this report covers the "grid," a North American system comprising the US, Canada, and a small part of Mexico.) On the cyber side, the focus was on the larger networks, including those that interconnect a company's information and operation systems and those that interconnect company systems to each other (Figures A-6 and A-7).

The most significant physical vulnerabilities appear to be related to substations, although certain generation facilities and transmission lines are also inviting targets. There is general agreement that since the industry designs for stability during single and certain double failures, a coordinated attack on multiple targets would be required to cause a significant disruption of service. Furthermore, such an attack would need to hit multiple targets simultaneously or in rapid sequence.

Because of the complexity of the grid, attackers would have difficulty replicating cascading outages such as the two western power outages of July and August 1996. More research is needed to better understand the dynamics of the grid, particularly the phenomenon of voltage collapse, which can lead to a cascading outage.

From the cyber perspective, SCADA systems offer some of the most attractive targets to disgruntled insiders and saboteurs intent on triggering a catastrophic event. With the exponential growth of information system networks that interconnect the business, administrative, and operational systems, significant disruption would result if an intruder were able to access a SCADA system and modify the data used for operational decisions, or modify programs that control critical industry equipment or the data reported to control centers.

Oil and Gas Vulnerabilities

Large refineries (greater than 250,000 barrel capacity) in California, Texas and Louisiana would be attractive targets for physical or cyber attack. The significant increase in the proportion of oil transported via pipelines over the last decade provides a huge, attractive, and largely unprotected target array for saboteurs. Elements of the pipeline system that could be targeted include lines at

river crossings, interconnects, valves, pumps, and compressors. Three major pipelines in the country offer the greatest potential for significant impact if attacked successfully. However, on the positive side, over the last five years, many interconnections have been added to natural gas pipelines, making rerouting around a break easier, but this may not always be possible if the line is at capacity.

As in the electric power industry, SCADA systems used in the oil and gas industries are subject to electronic intrusion. If accessed, information could be manipulated or control programs modified. Under certain circumstances, a hammering effect could then be induced in pipelines, possibly leading to breaks. More research is needed to determine the feasibility of such attacks.

Status and Assessment of Current Energy Infrastructure Assurance Programs

The DOE is the lead federal government organization for response to energy emergencies but has limited authority in the infrastructure assurance area. The Federal Energy Regulatory Commission (FERC) oversees wholesale electric and gas rates and service standards, as well as the transmission of electricity and gas in interstate commerce. The North American Electric Reliability Council (NERC) has assumed primary private sector responsibility for the reliability of the bulk power system (that is, the portion of the electric utility system that encompasses the electrical generation resources and transmission system shown in Figure A-1). The Security Committee of the Edison Electric Institute (EEI) provides a forum with a focus toward physical security and law enforcement activities for the security directors of investor owned utilities. The National Petroleum Council (NPC) is an advisory committee of 175 CEOs from the oil and gas industries, and the American Petroleum Institute's (API) and American Gas Association's (AGA) Telecommunications Committees provide forums for telecommunications specialists. The Electric Power Research Institute (EPRI), the Gas Research Institute (GRI), and the Institute of Gas Technology (IGT) are the leading energy technology organizations. The DOE National Laboratories are another source of significant expertise for solutions to the complex technical problems associated with infrastructure assurance.

As a result of the restructuring of the electric power industry, NERC has made significant changes to its organization, including the new requirement of mandatory compliance to its policies and procedures, compliance monitoring, enforcement measures, and increased and broadened membership. However, since NERC is a voluntary organization, enforcement is questionable. Also, a tension exists between different industry groups.

Another notable effort is the Secretary of Energy's Task Force on Electric System Reliability, which was recently established to provide advice on ways to address key institutional, technical, and policy issues associated with maintaining bulk electric system reliability in the new era of a competitive electric industry. An interim report, published in July, focuses on institutional recommendations to enhance overall reliability of the electric power system.

The critical components of the energy infrastructure remain vulnerable to physical attack, and replacement of many of these components involves lead times measured in months. However, most major companies have improved the physical security of their critical sites. From a cost benefit perspective, the companies believe they have taken prudent measures. Many companies' restoration programs are tested all too frequently by nature (hurricanes, earthquakes, tornadoes, fires, and floods) and existing mutual aid agreements have enabled restoration of service in reasonable time, even after the worst disasters.

From the cyber perspective, much needs to be done, and many issues have arisen, of which there is only limited awareness. Even the leading companies have only recently focused on information assurance issues. Despite increasing concern about vulnerabilities, many companies are understaffed in the cyber security area. Where cyber security experts are employed, their main focus appears to be on the business data processing side of the company, with a large share of their effort being expended on virus contamination problems. In most companies, information systems (business, administrative, and operations) are being networked, both internally and externally. Although many industry officials are aware of the significant vulnerabilities introduced by connecting to the Internet, most companies are making such connections. However, in attempts to provide security for information systems, many companies are placing confidence in individual measures, such as firewalls and dial-back modems, to secure their networks. The Commission's studies show that a more systematic approach is needed.

Several proactive information assurance efforts should be noted. The NERC has recently undertaken an initiative to collect information on cyber intrusions. EEI has volunteered to work with other interested groups to further scope the issues and activities in the cyber security area of the electric power infrastructure. EPRI has taken the lead in cyber security for the electric power industry, while DOE has assumed the lead for the federal government. For example, EPRI and DOE have joined forces to assess the security design and development of the information system of the Independent System Operator recently established in California. Also, DOE's Office of Nonproliferation and National Security has outreach programs on cyber security, energy emergencies, and threat assessments. Another notable effort was the three day seminar conducted by IGT (Emergency Response and Critical Infrastructure Protection in the Gas and Electric Industries) in June 1997.

Findings

1) The authorities and responsibilities for energy infrastructure assurance in the federal government need to be clarified.

2) The respective responsibilities of government and private sector for infrastructure assurance are not clearly understood.

3) Improved sharing of threat information and "indications and warning" (I&W) information is needed. Improved sharing of industry experience is needed (e.g., a fully populated cyber intrusion database).

4) More training and awareness in infrastructure assurance is needed, focusing on risk management, vulnerabilities, performance testing, and cyber security.

5) Infrastructure assurance technology advancements could add significantly to the overall protection of industry assets.

6) Adopting uniform physical and cyber security guidelines, standards or best practices would enhance protection.

Recommendations

Energy Infrastructure Assurance Strategy

Historically, the energy infrastructure's strategy has focused on robustness and resilience. The physical vulnerabilities of the pipelines and transmission grid are widely acknowledged and understood, and the philosophy has been to mitigate the natural and man made events that can exploit those vulnerabilities so that service to the customer is not interrupted or, if interrupted, only for the shortest possible time. To assure the energy infrastructure in the future, owners, operators, and the government must work together to develop a strategy focused on the primary objectives of prevention, mitigation and recovery.

Owners and operators can further expand communication channels with the government for sharing information on threats and vulnerabilities to ensure that they are making informed risk management decisions; enhance their research and development, focusing on cyber security and reliability projects; and as major customers of the telecommunications and software industries, make demands for more secure products and services.

Government agencies can contribute to the prevention, mitigation, and recovery of infrastructure losses by assuring that appropriate information sharing paths are established between owners/operators and the government; that existing or new regulations do not adversely impact the protection of the infrastructure; that a level playing field exists for the industry to invest in long term preventive measures; that threat and vulnerability information is provided to assist industry in making informed risk management decisions; and that long-term research and development activities are conducted to enhance assurance.

Implementation of Assurance Strategies

The Commission recommends:

1) Expanded roles and responsibilities for owners and operators, and the government to provide balance for the recommended strategy.

Owners and Operators

- Provide CEO level advisory counsel on infrastructure assurance issues, much as NSTAC provides advice for telecommunications. Representation could come from EEI and NPC.

- Provide threat dissemination and information sharing through associations such as NERC, API, INGAA and AGA.
- Formalize cyber security activities through such organizations as EEI, NERC, EPRI, API, and AGA.
- Fund enhanced infrastructure assurance near-term R&D through such institutions as EPRI and GRI.
- Emphasize education, training, and awareness using such resources as NERC and IGT.
- Provide a forum for development of enhanced physical and cyber security standards/guidelines through such organizations as the Institute of Electrical and Electronics Engineers (IEEE).

Federal Government

- Provide national direction through planning, policy, and legislation to maintain a level playing field for owners and operators investing in infrastructure assurance. Emphasize technology research, training and awareness, emergency response, and information sharing efforts.
- Develop and promulgate a mandated energy infrastructure assurance mission for the Department of Energy to address the responsibilities of the leadership and coordinating role as a federal government lead agency.
- Clarify the respective roles and responsibilities for pipeline security between the Departments of Energy and Transportation (DOT) through a joint effort.
- Provide enforcement/oversight for industry (electric power) reliability standards through FERC.
- Direct and fund the DOE National Laboratories to focus their expertise on infrastructure assurance assessments, response, and energy infrastructure assurance research and development (R&D).
- Expand the existing process for reporting power outages and physical attacks to include cyber attacks, and develop a legislative process to protect sensitive industry data.
- Develop and coordinate an enhanced process for timely, detailed threat information dissemination through the law enforcement and intelligence communities.

State Governments

- Provide assistance in the areas of training and awareness, and assurance exercises.
- Encourage the National Association of Regulatory Utility Commissioners (NARUC) to work through its member state commissions to enhance the protection of public utility infrastructures.

2) Owners, operators, and the government increase funding for R&D in the following technology related areas with security dimensions.
   - Cascading effects leading to voltage collapse.
   - Online security assessment, including online power flow and transient analysis.
   - Transmission and distribution technology, and real time control mechanisms.

- Large scale modeling and evaluation of the power grid and pipeline systems (regional and nationwide).
- Examine solutions to foreign energy supply vulnerability as a cost-benefit approach.

3) Secretary of Energy provide planning, policy, coordination, technical expertise and training/awareness for infrastructure assurance by:
   - Developing an energy infrastructure assurance plan in a coordinated government/private sector forum.
   - Encouraging development of physical and cyber security standards/best practices within the industries through the various associations (NERC, EEI, EPRI, IEEE, GRI, AGA, and API).
   - Developing and enhancing training, education and awareness programs for energy infrastructure assurance practitioners.
   - Providing the technical capability for vulnerability assessments available from National Laboratories to conduct reviews of critical infrastructure assets.
   - Funding a test bed/pilot program for energy infrastructure assurance that includes the private sector and government.
   - Coordinating with the private sector and DoD on research and development of risk management software and techniques, information assurance software and hardware for real time intrusion detection, enhanced authentication and authorization, and vulnerability assessment tools with a focus on SCADA systems.
   - Lead an industry/government effort to define the level of threat (e.g., criminal, insider, experienced hacker with intrusion software development capability) to be established as a goal for industry to defend against.

4) The Commission recognizes the importance of the following industry recommendations and recommends the Secretary of Energy work with the industry to:
   - Establish standards for a national "one call" program to address third party interruptions (dig-ins).
   - Continue joint effort between federal government, EEI, EPRI, NERC, and the oil and gas industries to further develop issues and activities pertinent to cyber security.
   - Review government regulations that require excessive reporting and release of what industry considers sensitive information (e.g., FERC Form 715 — Annual Transmission Planning and Evaluation Report).
   - Review regulations that may inhibit efforts by utilities to aid one another in emergency response efforts.
   - Form a permanently staffed center, jointly supported by government and industry, for sharing threat and vulnerability information from both public and private sector sources.

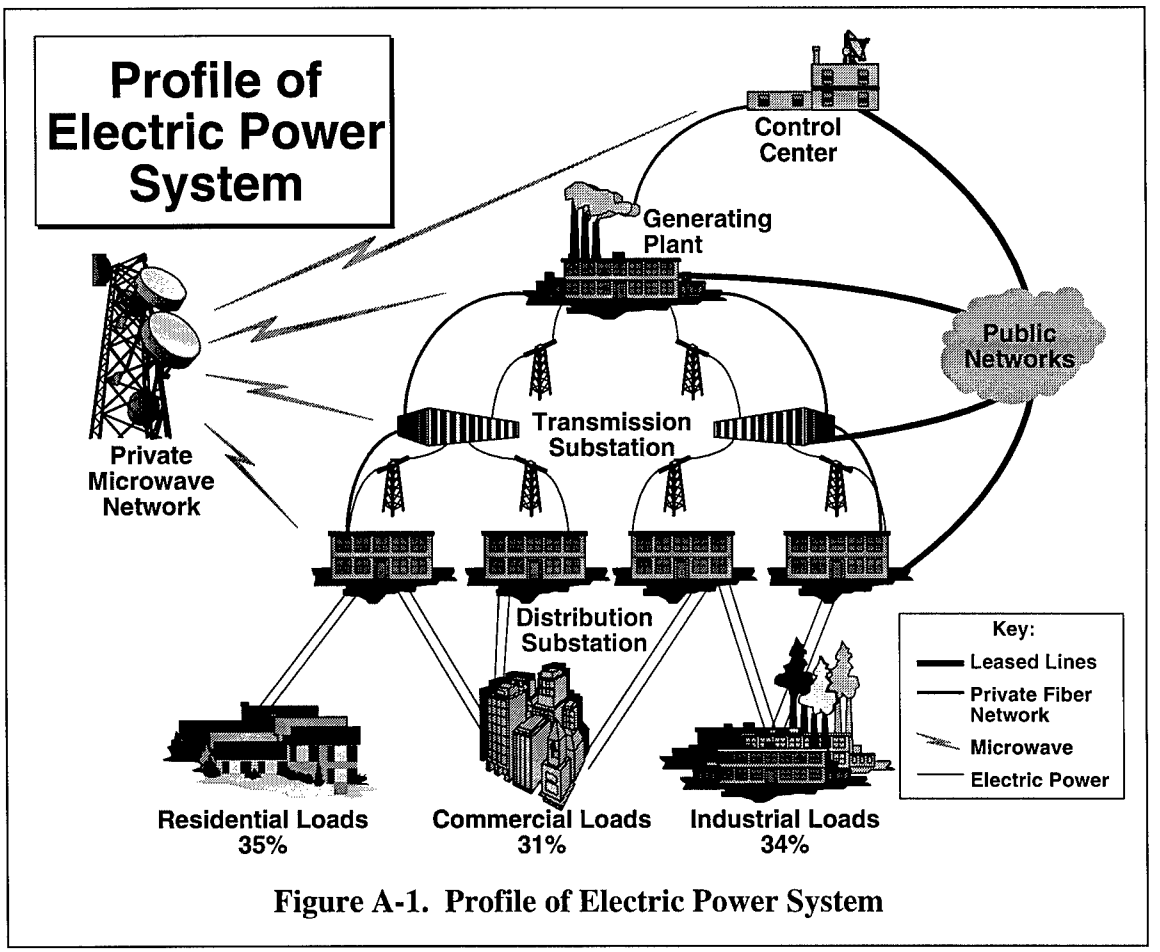


Figure A-1. Profile of Electric Power System

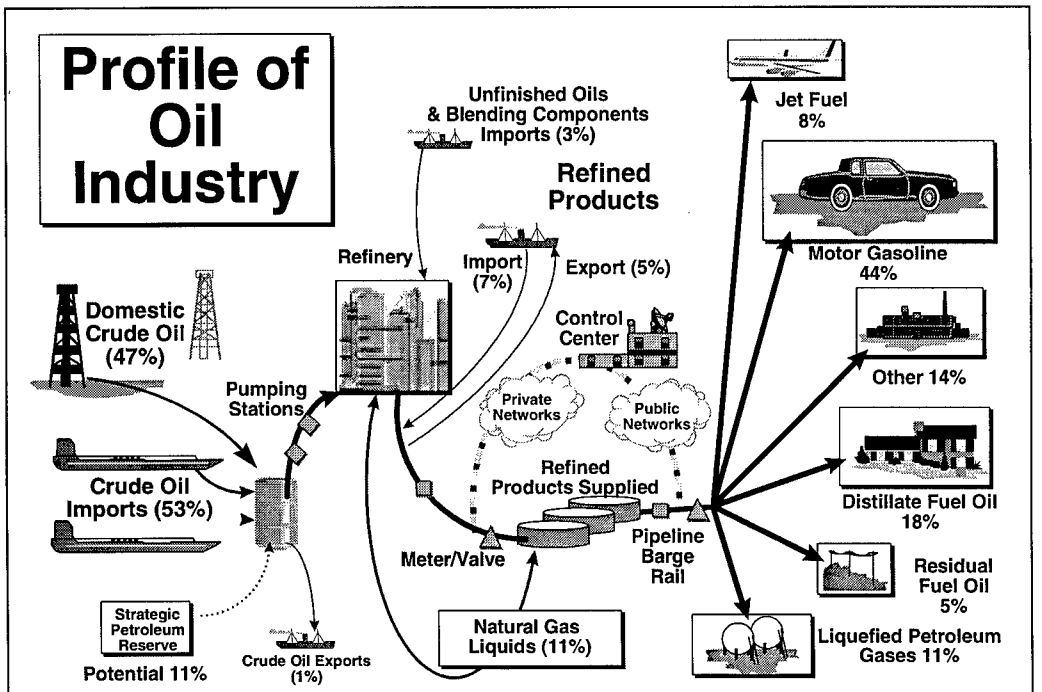


Figure A-2. Profile of Oil Industry

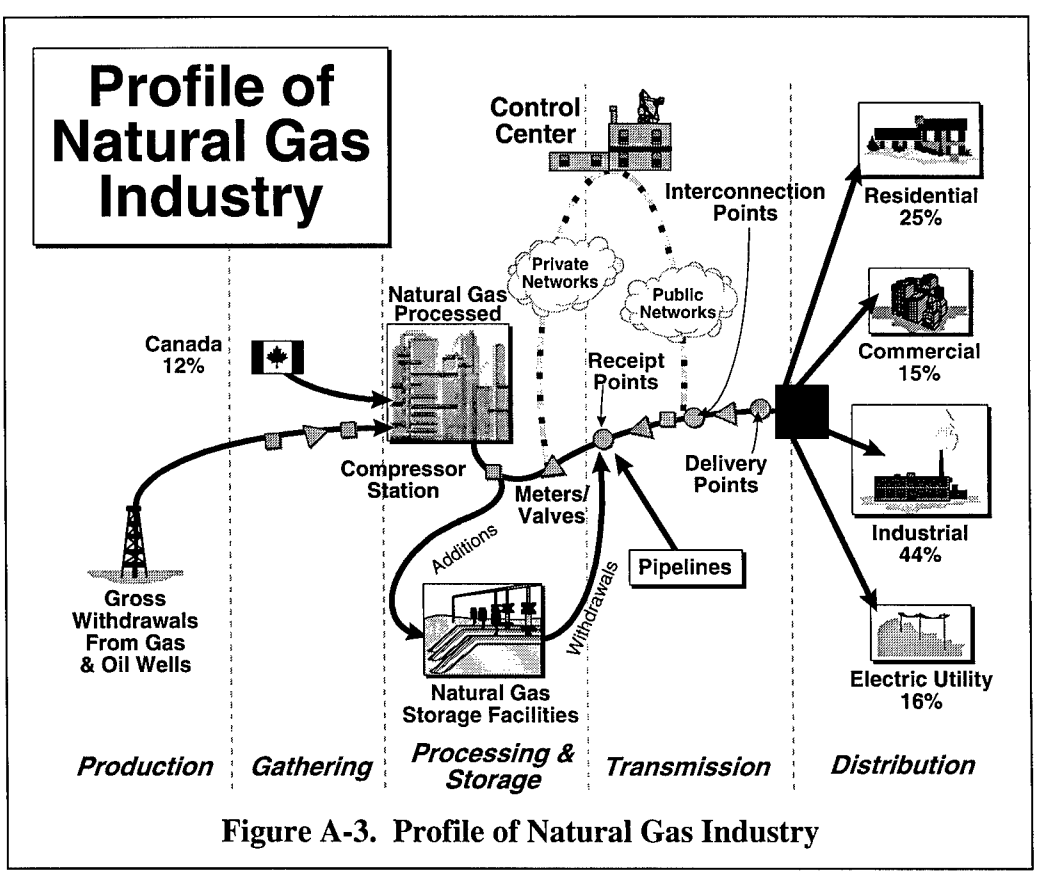


Figure A-3. Profile of Natural Gas Industry

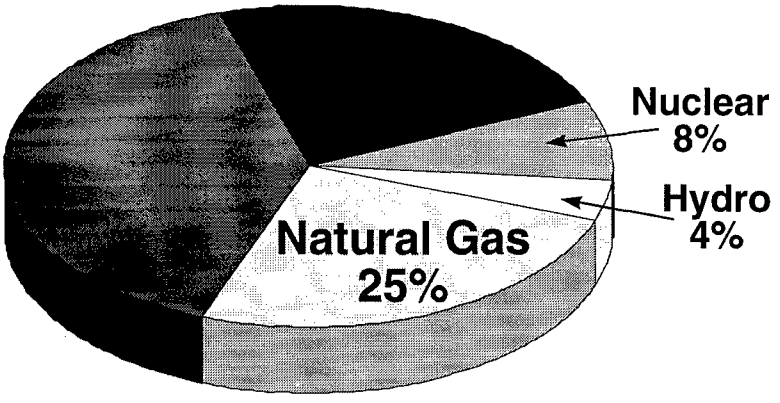
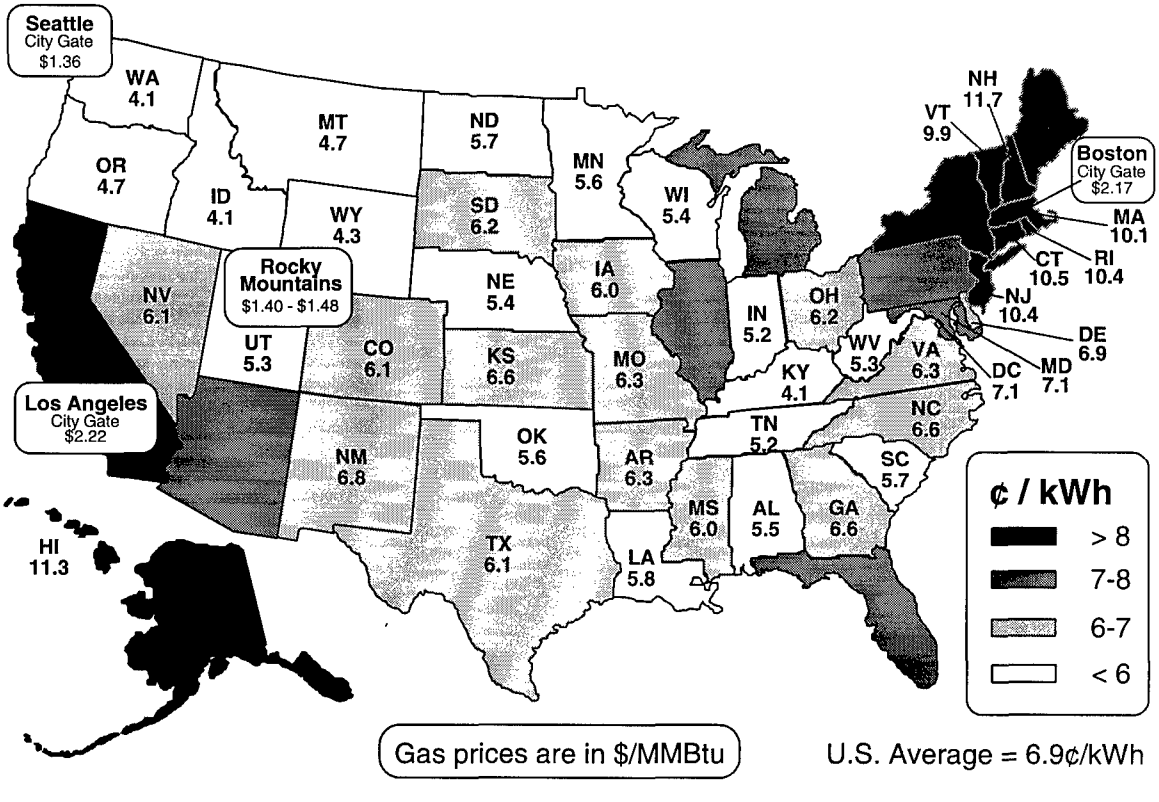


Figure A-4. US Energy Consumption



Source: U.S. Department of Energy, Energy Information Administration, DOE/EIA-0562 (96) and DOE/EIA-0348(95)/2 .

Figure A-5. US Electric and Natural Gas Prices

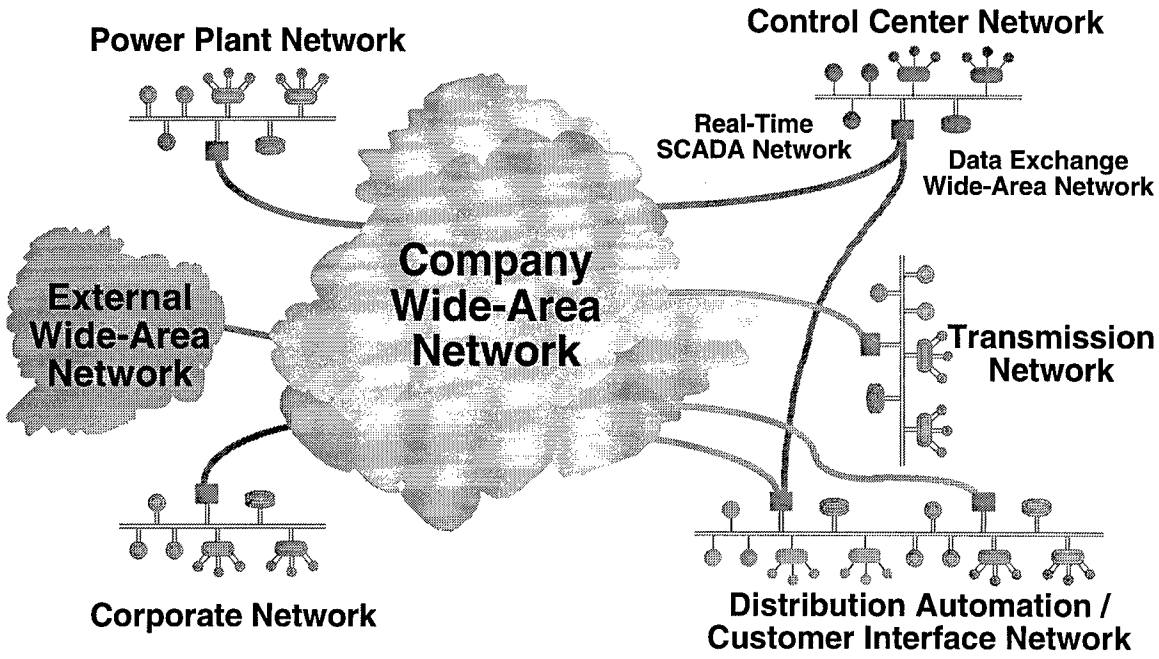


Figure A-6. Integrated Utility Network

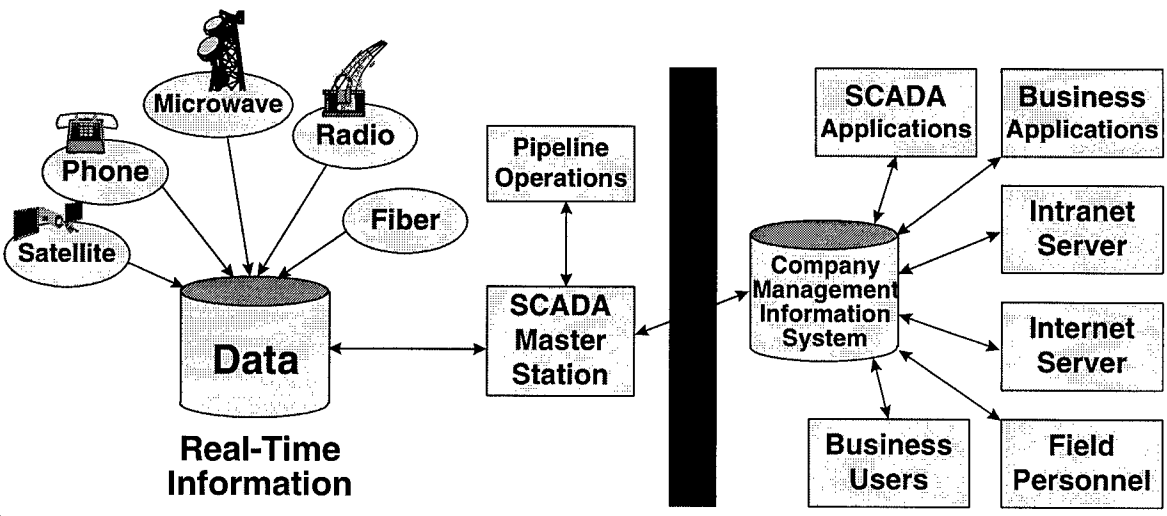


Figure A-7. Oil/Gas Current Internal System Configuration

Banking and Finance

Introduction

The US financial system is central not only to the functioning of domestic and global commerce, but to the daily lives of virtually all Americans. It represents bank holdings of about $4.5 trillion, a capital market of $7 trillion, investment bank underwriting of $1 trillion, almost $3 trillion in daily payment transactions, and about 10 million jobs.

More than a billion credit cards in circulation in the United Stated account for $500 billion in annual expenditure, or roughly half of all consumer debt. Also, due to the rapid increase in individual retirement accounts of various kinds and the popularity of mutual funds, about half of all households in the United States are investors in the stock market.

The banking and finance infrastructure was defined by the Commission as composed of five principal sectors: banks, financial service companies, payment systems, investment companies, and securities and commodities exchanges. The Commission's banking and finance team conducted a broad-based industry outreach, developed a profile of major participants, geographically mapped industry operations, assessed the level of vulnerability and defense extant within the financial system, and reviewed the analytic structures in prevalent use for such key industry processes as risk analysis and countermeasure investment decision-making.

Our principal finding is that, due to its carefully structured mixture of public oversight and private initiative, the US financial system is among the world's finest. The modern US financial system never has suffered a debilitating catastrophe, and for that reason among others carries an extraordinarily high level of global confidence. Some observers go so far as to characterize it as shock proof.

The Current Situation

The institutions comprising the financial services industry are further ahead than most in employing sophisticated and, in some cases, unique defenses against loss of assets and corruption of core data systems. Consequently, the US financial system is unusually well protected at the national level, and is well prepared to confront a broad range of threats to its operations and integrity.

However, along with other infrastructures studied by the Commission, the banking and financial service industry is undergoing significant structural change. Expansion by banks into previously prohibited business areas such as securities trading; mergers and acquisition activity; heavy and

growing engagement in dynamic global financial markets; and the steady move toward electronic commerce combine to present new challenges to the ways vulnerabilities are defined and risks and managed. And, at the operating level, heightened reliance on global information infrastructures and the advanced computing technologies which power them makes the management of those risks more complex.

Deregulation within the telecommunications and electric power industries upon which financial services so heavily rely introduces new factors to the industry's traditional risk management models. Multiple intermediaries have been inserted into what once were end-to-end service systems that—when combined with decreases in reserve capacity margins in these industries resulting from competitive cost pressures—make the operational interdependency among these three gigantic infrastructures even more opaque and complicated.

Risk Management

Managing risk is the principal business of financial institutions. They view protection against physical and cyber threats as a necessary cost of doing business, and they often position security as a competitive advantage and highlight it in advertising designed to attract new customers for such services as remote banking. Security is an integral component of institutional performance and accountability.

Security investments by financial institutions are driven by two primary forces.

- Law and Regulation: Mandatory investments made by the institution for legal or regulatory compliance. Because financial institutions are so heavily regulated, examination processes drive most security investments.
- Risk Management Analyses: Based on internal and external audit findings, industry and technology norms, history and current events, and estimates of future technology or threats, institutions evaluate risk according to probability of occurrence and the likely consequences for the institution. Security investments are made accordingly.

To assist in broadening the industry's recognition of new threats and vulnerabilities that could affect their risk assessments, financial institutions would benefit from better access to reliable current information from government and from across the industry. Reporting is generally compartmentalized by sector; only a few trusted mechanisms now exist for sharing the kinds of information needed to facilitate system-wide risk assessments.

Threats

The major current threats to the overall operation of the financial system are largely physical in nature, consisting either of natural disasters or a direct coordinated attack on the system's more vulnerable points. These are aggravated by the more open availability on the Internet of the kind

of information needed to plan such attacks, increasing reliance on global outsourcing of core operations, and the consolidation of bank and other operations centers as a result of merger and acquisition activity.

At the institutional level, however, the most persistent security threat is the insider who might use authorized access to confidential information or operating systems for profit. Financial institutions employ comprehensive and intricate systems of internal controls to counter this threat, but the knowledgeable insider dedicated to corruption is difficult to stop.

There is also the evolving threat of a larger scale cyber attack by a sovereign adversary or organized terrorists with the aim of inflicting serious damage on key elements of the US financial system. The current probability of this threat is estimated to be low but growing, and one of its more troubling features is that its source may be undetectable and the attack itself might be masked as a series of lesser intrusions.

Vulnerabilities

It is important to note some key distinctions in describing financial system vulnerabilities.

First, there is the distinction between vulnerability of the US financial system and opportunities for theft and fraud in individual institutions. Almost all media reporting on vulnerability up to now has risen from single cases of theft. Emblematic of this is the much reported access of Citicorp's electronic money transfer operation by a transnational criminal group in 1994. While this case made dramatic news accounts and was embarrassing to Citicorp, whose ultimate loss amounted to $400,000, it in no way reached the level of a threat to the bank, much less the financial system.

Second, there is the distinction between the financial condition of a single participant in the financial system and the strength of the system as a whole. Recent years have seen some spectacular financial events, such as the Mexican Peso crisis, the failure of Barings Bank due to fraud, and major scandals involving Japanese banks. These shocks were absorbed and managed by appropriate market, regulatory, and central bank actions without lasting harm to the full system.

Based on the sector profiles developed by the Commission, the nation's core payment systems (FedWire, CHIPS, SWIFT) and the organized securities and commodities exchanges seem to present a serious physical vulnerability within the financial system. This is so not because they have failed to take extensive precautionary measures, but rather because there is substantial cross sector dependence on the services they provide, and few if any alternatives available to provide those services in the event of a disabling catastrophe. In contrast, our analysis shows that the other sectors of the financial infrastructure have sufficient diversity to provide for the dispersion of risk among a wide range of alternatives.

As a countermeasure, the FedWire, for example, maintains three hardened operating centers capable of carrying the full volume of its wire transactions. Similarly, the New York Stock

Exchange (NYSE), as the nation's most influential exchange, has established extensive system redundancy, alternate power sources, and diverse communication links. Still, the physical concentration of its data processing and operations centers makes more plausible the possibility of an event or series of events that could disable both sites. Even in that event, however, contingency trading arrangements required by the Securities and Exchange Commission (SEC), although never tested, have been described by the SEC as able to restore NYSE operations within several days. Other major exchanges, such as the Chicago Board of Trade and the Chicago Mercantile Exchange, have similar recovery plans, as do lesser securities exchanges.

Public Confidence

Financial institutions are acutely aware that public confidence is their most critical asset. In that respect, the financial service industry shares with government a fundamental dependence on public support for its viability. This linkage is the basis for the important role government has in assuring the safety and soundness of US financial system.

Because of its sensitivity, however, financial institutions generally oppose reporting which goes beyond the existing mandatory regulatory and law enforcement channels. While it is understandable that these institutions wish to avoid costly reporting requirements and potentially damaging disclosures, taking such a position fuels critics who claim that there are large unreported losses -- especially related to computer intrusions of various kinds. Any new mechanism for the exchange of information must establish an acceptable climate of trust and control which will encourage participation by financial institutions yet meet emerging governmental national security requirements for more coherent, systemic risk assessments.

Market Forces and Government Action

There is little doubt that ultimately market forces will generate the appropriate level of investment in risk management tools necessary to secure the financial infrastructure into the future. Nevertheless, the financial system regulatory changes under consideration by the Administration and Congress all have in common an important government role in setting ground rules for new forms of competition; providing a level of fundamental indemnity for customers of the system, thereby relieving companies of some risk; and protecting the public interest in the safety, soundness, and fairness of the system as a whole.

Market forces work best when businesses see the investment as a necessary cost of operation, as consistent with their concepts of risk, as providing a competitive advantage, and protecting their brand (Figure A-8 illustrates this process). In this context, one of the problems with sole reliance on market forces for long-term investments in research and development of security tools, for example, is the lack of actuarial data upon which the risks associated with new threats and vulnerabilities might be calculated. Neither can the benefits of the investment be specified. Consequently, the economics of long term prevention measures often works against their development.

For example, for such major preventive measures as the establishment of redundant communications systems for the industry to rely on in the event of a catastrophic telecommunications or electric power failure, or the construction of an alternate trading site for the securities exchanges, payoffs are not easily envisioned. In the absence of measurable risk, the net present value of such investments is minimal if not zero, and justifying present costs to shareholders, investors, and securities analysts by citing general benefits in the absence of clear risk or competitive advantage is not likely to succeed. Therefore, business on its own will not invest in the kind of ultra secure contingency measures usually found in the military or national security arena without either more information about the risk, or some other incentive.

Summary

The current security of the US banking and finance infrastructure is strong. The government, through regulation, plays a central role in assuring the financial system's safety, soundness, and fairness, but the industry itself has over many years developed a diligent culture of security. Both the role of government and industry diligence will continue even as governing statutes and regulations are changed, technology advances, and the industry restructures and competes in the global market.

However, it is important to note that scrutiny of the financial services industry goes beyond government regulation and law enforcement. Because of its centrality to the nation's economy and the daily lives of most Americans, the extraordinarily high value of its assets, and its high global visibility, the industry's operations and behavior are closely observed by securities analysts, investors, major customers, journalists, and the public in general. This provides powerful additional incentive for financial institutions to assure their integrity and take the actions necessary to continue to earn and retain broad public confidence, retain customers, and achieve growth.

Overall, industry risk management efforts concentrate on prevention of loss, with mitigation of loss following in importance. However, contingency planning also is a high priority, as disablement resulting from an attack or natural disaster remains the industry's largest current risk.

Cyber risks on a system-wide scale may emerge from the possibility of unforeseen instability in the telecommunications and electric power industries as they deregulate and disaggregate. On an institutional level, increasing use of electronic banking mechanisms, requiring multiple ports of entry and perhaps an entirely new infrastructure to accommodate the demand for rapid data recall and payment processing, will create new forms of risk to information systems. For example, connections to the Internet for this purpose present a risk of unauthorized access to operating systems if the Internet connection is not effectively partitioned by firewalls and other such tools. Banks and others are approaching this with caution, although the attraction is strong in terms of operational efficiency and expanded market reach.

In the longer term, risk emerges from the maturing of Information Warfare capability among organized adversaries who may wish to attack the US by destabilizing large portions of the finan-

cial system, and erode public confidence in it as well as in the capability of the US to defend against such attacks. Both the government and industry would significantly benefit from improved flows of threat and vulnerability information so that precautionary measures can be developed and deployed system-wide at a pace sufficient to provide an effective defense.

Recommendations

Information Sharing

Regulators, law enforcement officials, and industry associations should coalesce to establish a trusted forum for the exchange of relevant threat and vulnerability information so as to facilitate the assessment of risk on a system-wide basis.

Contingency Planning

Regulators and industry associations should sponsor strategic simulations designed to test the adequacy of existing industry recovery plans under a variety of conditions. These should feature the emerging risk factors of growing interdependence complicated by deregulation and global expansion of operations.

Insider Threat

Regulators, private auditors, and the industry should continue to work together to improve examination processes, audit practices, internal controls, and physical security measures to accommodate new kinds of risks and to help deter the insider threat.

Back-up Facilities

National security, law enforcement, and regulators should decide whether the establishment of such security measures as a contingency trading site for major exchanges, contingency data storage centers, and dedicated communications systems, the cost of which probably exceeds the reasonable business risk involved, are appropriate as government-funded national security measures.

Education

Industry associations may wish to take the lead in establishing information security education and awareness programs within academia and in the general public.

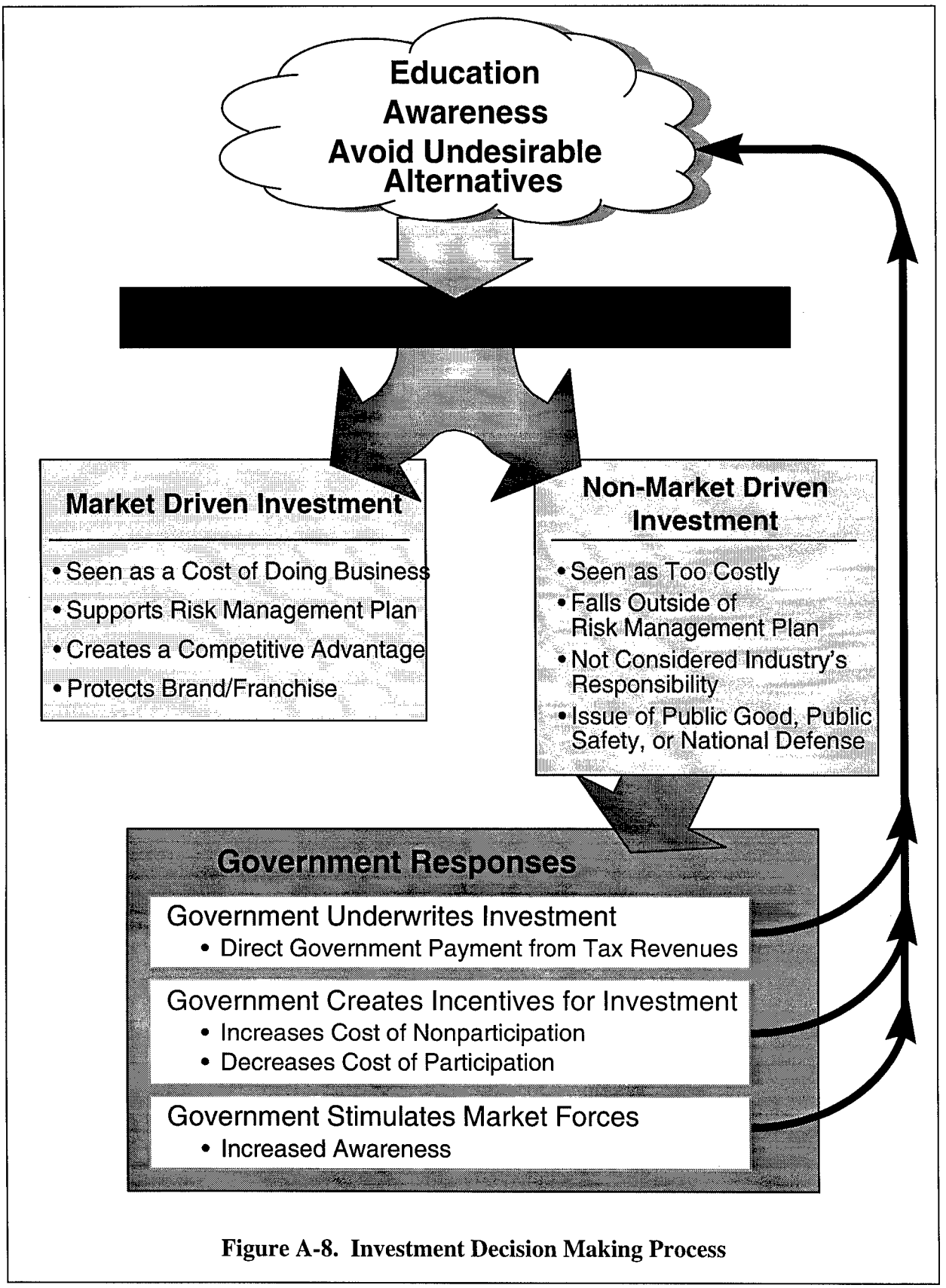


Figure A-8. Investment Decision Making Process

Vital Human Services

Introduction

The Vital Human Services (VHS) sector includes three of the critical infrastructures named in Executive Order 13010: water supply, emergency services, and government services. At the outset, the Commission considered expanding the scope of this sector to include food, health care and the nation's work force as additional critical infrastructures. However, because of time and resource constraints, the Commission decided to bound the scope of its effort to the eight infrastructures named in the Executive Order, leaving additional infrastructures to be considered in any follow-on activity.

The three VHS infrastructures differ from other named critical infrastructures in that they are focused largely at the local and state levels, are largely governmental responsibilities, and deal chiefly with human needs and safety. Because they are highly localized in character, they do not form a strongly interconnected national infrastructure. Failures in one community generally will be localized to that community. Nevertheless, they are critical national infrastructures and the problems and vulnerabilities faced in one community are similar to those faced in every community across the US.

Because these infrastructures relate directly to the populace, their disruption—or even threatened disruption—would have significant psycho-social effects. Loss of confidence in these infrastructures can greatly magnify the more objective costs to the economy and national security.

Water Supply

There is no "typical" water supply system for the US, at least not to any significant degree of detail. But, at a general level, all systems share five common elements.

1) A water source, either surface waters in impoundments such as lakes and reservoirs or flowing waters in rivers or ground water in aquifers.
2) Treatment facilities in which particulates are filtered out and disinfectants are added.
3) A system of aqueducts, tunnels, reservoirs, and/or pumping facilities to convey water from the source through the rest of the system and to provide storage and the means to balance flows.
4) A distribution system carrying finished water to users through a system of water mains and subsidiary pipes.
5) A waste water collection and treatment system.

The major uses of the water supply infrastructure are for agriculture, industry (including various manufacturing processes, power generation and cooling), business, fire fighting and residential purposes. In many cases, the water supplies for agriculture and industry come from outside the public water supply system, being drawn by the users directly from surface or ground sources. However, in some areas, such users are dependent upon public water supply and for them a failure of the public system could be devastating. Small communities and rural residents often are not served by a public water supply system. Instead, they either have their own wells or are served by private water systems.

Three attributes are crucial to water supply users. There must be water on demand; it must be delivered at sufficient pressure; and it must be safe for use. Actions that affect any of these three factors can be debilitating for the infrastructure.

Contamination of potable water supplies occurs occasionally by accident or from natural causes. Natural blooms of parasites such as Giardia and Cryptosporidium have occurred in many water systems. Such parasites are resistant to treatment with chlorine and therefore require the user to boil water before ingesting it. These blooms are sometimes related to feed lot runoff (the parasites are prolific in the fecal material of farm animals). Naturally occurring blooms generally last for a few days or weeks and then disappear. Some experts voice concern that these parasites, and possibly others, could be introduced deliberately into water systems and cause illness and death in great numbers before the situation could be remedied.

Many common organisms such as *e.coli* are destroyed in the normal water supply environment. An appropriate acidity level (pH) and oxidant level (e.g., chlorine) can destroy many such organisms in less time than they typically remain within the flowing water system. However, there may be bacteria, viruses and other pathogens that can survive this environment to cause sickness and death among the served population. The Commission concluded that there is a credible threat to the nation's water supply systems from certain known biological agents, and that for many potential agents, there is a serious dearth of scientific knowledge needed to assess their threat potential. In addition, there are newly discovered pathogens that emerge under conditions of very high nutrient burden, a condition increasingly common in today's agricultural environment, and their properties are even less well known or understood.

Chemical contamination is also of concern. Several chemical agents have been identified that would constitute credible threats against water supply systems. Although much is known about chemical and biological agents dispersed in air, almost no work has been done on potable waterborne agents. Natural contamination has occurred from surface run off, leaching from toxic waste dumps, or toxic materials, leaking from underground pipes and tanks. These accidental contamination incidents generally have been contained or dealt with successfully.

We have seen no persuasive evidence that purposeful radiological contamination of public water supply systems constitutes an important threat.

The amounts of material needed for purposeful contamination of a water source (such as a large reservoir or aquifer) are considerable and exceed what an individual or small group of terrorists

could easily transport. However, contaminants introduced later would be less susceptible to dilution and would reside in the system for shorter times, thus diminishing the effects of disinfectants and chemical decomposition and oxidation.

Loss of water or water pressure can result from a number of causes. For example, disabling the pumps that maintain flow and pressure, or disabling the electric power sources that run them, could cause long term outages since many of the major pumps and power sources are unique, custom designed equipment that would take months or longer to replace. Fitting more readily available replacement elements might be possible in some situations; however, in several instances we were informed that the engineering difficulties would be serious and that down time would still be on the order of months.

Public potable water systems supply the water for fire fighting in most communities. Loss of water, or even substantial loss of pressure, would disable most fire fighting capability. Some communities have the ability to tap other water sources for fire fighting. For example, fires in Manhattan could be fought by New York's fireboat fleet drawing water from the East River or the Hudson River. Some communities, such as Los Angeles, have large mobile water tankers strategically placed and available to fight fires in case the water system is disabled; the main concern there being earthquakes. Such planning appropriate for natural disasters is largely translatable to other risks. Some communities have mobile pumpers that can withdraw water from storage areas or natural bodies and make it available for fire fighting. Such capabilities, however, are available to only a few cities. Limited capabilities exist to draw water from saltwater sources and transport it to the site of fires. This capability has been used in fighting forest fires in remote locations and probably would be available to urban communities if needed.

Many urban water systems have to rely on a fragile distribution structure. Often referred to as an aging infrastructure, the real problem is that temperature variations, swings in water pressure, vibration from traffic or industrial processes, and accidents often result in broken water mains. Distribution systems in most major cities operate with very little margin. They plan on a number of main breaks based on historical experience. Coordinated attacks on a large number of water mains simultaneously would be difficult to carry out and are not a highly likely threat scenario. However, a system-wide water hammer effect, caused simply by opening or closing major control valves too rapidly, could result in a large number of simultaneous main breaks that exceed the system's capability to respond in a timely manner and would cause widespread outages throughout the community. Recognizing this vulnerability, water systems lately have been incorporating valves that are physically not possible to open or close rapidly. However, many urban systems still have in operation valves that could cause severe water hammer effects.

Finally, interrupting water flow to agricultural and industrial users could have large economic consequences. For example, the California aqueduct, which carries water from northern parts of the state into the Los Angeles/San Diego area, also serves to irrigate the agricultural areas in midstate. Pumping stations are used to maintain the flow of water over rises in terrain. Loss of irrigation water for a growing season, even in years of normal rainfall, would likely result in billions of dollars of loss to California and significant losses to US agricultural exports.

An ancillary problem concerns release of chlorine to the air. Most water supply systems use gaseous chlorine as a disinfectant. The chlorine is normally delivered and stored in railway tank cars. Generally, there is no protection against access to these cars except the overall facility security, which is more often than not minimal. Release of chlorine gas could cause injury to nearby populations.

Foreign ownership of US water supply systems is increasing. But we see no indication of an important vulnerability growing out of this trend.

To summarize, the major vulnerabilities of the nation's water supply systems include susceptibility to contamination and loss of flow and/or pressure resulting from extensive water main breaks, destruction of pumps, or disruption of power supplies.

Emergency Services

This infrastructure includes firefighting, police, rescue, and emergency medical services. Its objectives are to contain and deal with emergencies in order to save lives and preserve property. Except for certain parts of the emergency medical services element, this infrastructure is mostly government owned and operated. It is focused at the local level; state and federal services play an important but supporting role. The infrastructure as defined by the Commission does not include investigative or law enforcement functions, nor does it include activities in the recovery phase.

Local police, firefighting and emergency medical services are generally first on the scene of an incident involving public places. Incidents, including accidents, natural disasters, fires or physical attacks involving private facilities, usually are turned over quickly to the emergency services sector because private organizations generally lack the specialized training and resources necessary, and because there may be legal mandates, constraints or consequences of private action. Local authorities faced with large scale incidents turn, where necessary, first to neighboring jurisdictions with whom they have mutual aid agreements for assistance and then, if necessary, to the state. As a general rule, with few exceptions, federal authorities must be invited before they can play a role.

Because of their key role and because time is usually of the essence in dealing with emergencies, the inability of local responders to handle or contain an incident can be a serious vulnerability. It can greatly amplify the effect of the initial event. For example, the inability of a fire department to manage a fire could lead to its spreading and to increased loss of life and property.

The emergency services functions most susceptible to disruption include timely notification of an incident; dispatch of appropriate responders; access to the site; coordination among responders; and effective containment of the incident.

Timely Notification

The 911 system has become popular and is widely used. However, it is susceptible to overload, both by reporting of minor non-emergency incidents and through mischief or malice. There have been several instances where computer viruses that automatically and endlessly dial 911 have been distributed to unsuspecting users. At the programmed time, they flood the system so that it is inoperable. Also, because the system uses the public switched network (PSN) for telecommunications, failures in the PSN can also disable 911.

Fortunately, most major communities do not rely exclusively on the 911 system to provide notification of important incidents. In addition to having alternative telephone numbers, many systems also make use of routine patrols, surveillance (such as through the use of helicopters), reporting by traffic monitors, and even the news media.

Dispatch

In some communities, the dispatch function is centralized. If it is disabled, the ability to notify responders of an incident and to coordinate initial phases of the response is destroyed. Most large cities, however, have redundant and geographically separated dispatch capabilities.

Access to the Site

Traffic congestion in urban areas threatens the ability of emergency systems to respond to incidents. Despite laws and protocols designed to speed emergency responders to their destinations, the flow of traffic often is so heavy that responders suffer significant delays. As cited in the Physical Transportation section of this Appendix, several cities are developing or already using automated traffic control systems, called Intelligent Transportation Systems (ITS), that sense the traffic and control traffic lights to optimize flow and reduce congestion. Such systems can be used to facilitate access to incident sites. However, these advances are two edged: the same automatic system that can control traffic beneficially can be compromised to cause traffic tie-ups and block access by emergency vehicles. These systems appear to have been designed and installed with insufficient regard for security measures needed to prevent or deal with cyber attack.

Coordination

Effective communication among units responding to emergencies is essential for coordinating their efforts. Interoperable communications is needed among police and fire units, medical facilities, and utility or transportation repair crews; across all levels of government; and into the public telephone system. While a wide range of communication options is available, virtually all depend upon having sufficient access to radio frequencies. The bands of frequencies available for public safety are proving to be insufficient due to congestion or interference from other sources.

Today, several bands of radio frequencies are allocated specifically for emergency services, and other bands have been made available for temporary use. The Public Safety Wireless Advisory Committee (PSWAC) concluded in its final report that these existing bands are inadequate. Additional spectrum access is needed to relieve congestion in several urban areas; to facilitate interoperability between existing public safety communications systems; to mitigate interference

problems; and to support migration to modern communications capabilities. In addition, the Federal Communications Commission's (FCC) auctioning of certain frequency bands would force emergency services to move into other spectral ranges, primarily in the 800 MHz band. This would have several undesirable effects. The crowding can produce interference. It would make it easier to jam emergency communications. In cities where there is a high density of large buildings and subsurface systems such as subways, the 800 MHz band—whose signals cannot penetrate concrete and steel structures—is ineffective for emergency communications.

In response to a PSWAC recommendation, the President recently announced an FCC proposal to reallocate the 24 MHz of spectrum currently used by UHF television broadcast channels 63, 64, 68, and 69 for use in public safety communications. Unfortunately, the FCC proposal retains priority of spectrum use for existing and future DTV broadcast stations in these channels; public safety users will have to ensure they cause no interference to television broadcast. Under this proviso, these channels are effectively unavailable to public safety use in several major urban areas. Also, while the FCC's proposal meets the PSWAC recommendation for 24MHz to be made available immediately, it does not address the PSWAC recommendation for up to 66MHz of additional spectrum needed in the future.

Two other factors limit the implementation of interoperable emergency service communications. First, even if additional unencumbered spectrum is made available and a community wants to transition to new frequencies or adopt a new capability, the transition is likely to be costly. Communities faced with such costs may have no alternative but to migrate in stages, which would result in interoperability problems during the entire transition phase. Second, because emergency response in today's world may involve units drawn from a broad regional or even national cross section, interoperability is desirable among all responding units. Approaches will need to be harmonized, geographically across the nation as well as between levels of government. These two factors point to the need for a comprehensive *National Emergency Services Telecommunication Plan* to define common communications approaches, address the financial resources required for the transition, and outline the phasing to minimize interoperability problems during the transition.

Containment and Effectiveness

Based on discussions with local emergency services officials and with national associations, it is apparent that throughout the country there are few, if any, jurisdictions in which first responders feel adequately trained and equipped to meet chemical, biological or radiological incidents. They do not have sensors to tell them they are encountering offending agents or to identify the agent. They do not have adequate protective gear so they cannot be assured of their own safety in dealing with such an incident. They do not have decontamination equipment so they are not able to terminate their own exposure to the agent or that of victims, even after leaving the site. And they do not have sufficient supplies of atropine and other antidotes with which to treat themselves or members of the public who become exposed.

The federal government recognizes this need and provides a number of training and assistance programs for local responders. For example, the Nunn-Lugar-Domincci legislation provides significant funding for a well designed set of program efforts aimed at improving the ability of

local responders to deal with weapons of mass destruction (WMD) incidents. Such efforts need to be intensified and made more widely available more rapidly. Also, there needs to be put in place an affordable mechanism to continually upgrade local capabilities, tracking advances in the capabilities of adversaries.

Containment of fires (and certain other incidents) depends on the availability of water under sufficient pressure. Should the water supply system fail, precious minutes or hours could be lost while alternatives are made available; in most communities, there are no such alternatives.

Often, the federal government has information that can alert local officials to threatening situations and can assist them in preparing for and dealing with incidents. The sharing of information between local and federal levels has not been as effective as it could be. It needs to be improved.

Across the nation, there are federal facilities that have resources that could be important in dealing with emergencies. Traditionally, military base commanders readily provide such resources—food, medical supplies, transportation, manpower, etc.—when needed. However, federal organizations rarely (if ever) participate with nearby organizations in the planning phases of emergency response. This can be important in providing local responders a better understanding of gaps in response capability and procedures for activating federal responses.

Federal capabilities to deal with chemical, biological and radiological incidents are advanced but limited. They can be activated by request originating with the local incident manager, gaining the concurrence of the local mayor and the state governor, and passed along to the Defense Department's Director of Military Support (DOMS) organization. Upon approval, the support mission is assigned to the appropriate base commander, who then orders the unit into action. For planning purposes, it is assumed that a federal team can be on site within 7 to 10 hours after the local incident manager makes his request. There is little practical experience to validate this planning assumption, but given the delays possible in the process, it seems likely that the actual time required to arrive on station could exceed 12 hours. Saving lives in a chemical or biological attack requires a response on the order of minutes. Therefore, no matter how streamlined the activation process, the best solution would appear to be to have such capability at the ready, i.e., pre-positioned based on an expectation or indication of a threat.

In summary, the emergency services infrastructure, which depends heavily upon first responders' capabilities, has fundamental weaknesses that could be exploited to amplify the impact of attacks. These vulnerabilities of the infrastructure can be remedied through more extensive training; access to better technology; better sharing of information; and supplies of critical materiel.

Government Services

Executive Order 13010 designated "continuity of government" as a critical infrastructure. This term has traditionally applied to the survival of our Constitutional form of government in the face of a catastrophic crisis such as nuclear war. In January 1997, a memorandum to the Commission Chairman from the Acting Assistant to the President for National Security Affairs noted that this

traditional concept is distinct from the continuation, in the face of physical and cyber threats to our infrastructures, of services provided by federal, state, and local government. The memorandum stated that it was the latter problem that the Commission was expected to address. Consequently, the Commission has considered *government services* as a critical infrastructure.

Government serves several functions. At the federal level, the Constitution sets forth the responsibilities of government for establishing justice, ensuring domestic tranquillity, providing for the common defense, promoting the general welfare, and securing the blessings of liberty. The constitutions of the 50 sovereign states assign certain parallel responsibilities to the state and local levels. To fulfill these responsibilities, governments at all levels make use of organizations that develop policy, operate programs, regulate, exercise police powers, disburse funds to members of the public, collect taxes, etc. The Commission's focus is on those services of government that are, for the most part, oriented toward promoting the general welfare. This includes, but is not limited to, health and safety as well as disbursements.

Because of time and resource limitations, the Commission has not probed all of the federal, state and local governmental services included in this infrastructure. Emergency services have been dealt with as a separate infrastructure, and to gain an understanding of other government services we sampled Centers for Disease Control (CDC); Social Security Administration(SSA); National Weather Service (NWS); Immigration and Naturalization Service (INS); and state welfare systems.

From the sampled organizations, we draw the following conclusions.

- There is a strong trend toward increased dependency on computer technology, extensive automated databases, ties to the Internet and reliance on the global telecommunications network. Security considerations generally are not high priority.
- Most governmental databases (among government service organizations) contain information relating to individuals and companies and such information is subject to privacy constraints. Vulnerabilities of databases are most likely to be associated with alteration, destruction, or misuse of individual records rather than with global (that is, database wide) effects. At least in the organizations sampled, therefore, it appears very difficult for an outsider to affect more than a small number of records at a time.
- In some cases, physical vulnerabilities may be important.

At the federal government level, the Office of Management and Budget (OMB) has responsibility (under the Paperwork Reduction Act of 1980, as amended) to "develop and implement uniform and consistent information resources management policies; oversee the development and promote the use of information management principles, standards and guidelines; evaluate agency information resources management practices in order to determine their adequacy and efficiency; and determine compliance of such practices with the policies, principles, standards and guidelines promulgated by" OMB.

OMB Circular A-130, based on this legislative authority, directs all agencies to, *inter alia*, "protect government information commensurate with the risk and magnitude of harm that could

result from the loss, misuse or unauthorized access to or modification of such information." Agencies are also directed to appoint an individual responsible for strategic information resources management.

While the guidelines provided by OMB are sound, they have not been implemented widely throughout the government. Nor has OMB enforced them.

The National Institute for Standards and Technology (NIST) has the legislated authority to provide assistance in information security to the civilian agencies of the government while the National Security Agency (NSA) has that responsibility for the non-civilian agencies. NSA has pursued its charter enthusiastically and creatively. It has been relatively successful in its program. NIST, residing in a culture that emphasizes academic values and methods, has taken a less aggressive posture and has not obtained resources adequate to its legislated charter in this area. Nevertheless, NIST is developing a set of tests that can be employed to gauge whether information technology products meet certain security and suitability criteria, and has established a program to accredit testing laboratories conducting such tests.

Governments are important purchasers of information technology products. A procurement policy that insists that purchased products undergo rigorous testing and receive appropriate certification would go a long way toward encouraging the private sector to seek such tested and certified products as well.

Major Recommendations

We recommend that the federal role in assuring VHS infrastructures include the following:

- Performing and/or supporting a research and development program to develop needed scientific information on potential contaminants of water supply systems and technology to detect, identify, and treat affected water supply systems. Also, planning and researching on medical treatment of persons exposed to these contaminants through ingestion or absorption through the skin of waterborne agents.
- Providing training and certain equipment, particularly in dealing with chemical, biological and radiological incidents, for local first responders from all jurisdictions likely to face such threats.
- Collecting, analyzing and sharing information concerning threats and vulnerabilities.
- Providing an indications and warning (I&W) system that informs all participants in emergency response of imminent or expected threats and of attacks in progress.
- Raising the level of awareness of the public and of owners and operators of these infrastructures to both physical and cyber attack possibilities and system vulnerabilities, such as ITS vulnerabilities recommended in the Physical Transportation section of this Appendix.
- Making accessible to infrastructures all government owned technology of use in dealing with threats and vulnerabilities of infrastructures.

- Making accessible protective and decontamination gear to first responders.
- Making available stores of atropine and other antidotes.
- Providing information on the identity and location of supporting equipment and replacement equipment, manufacturers of assets at risk, and channels in which to communicate with them.
- Assisting in development of comprehensive Geographical Information Systems (GIS) systems at the local level.
- Encouraging federal government services to assess their vulnerabilities and incorporate adequate attention to security in all plans and operations.
- Ensuring adequate allocation of unencumbered electromagnetic spectrum for public safety telecommunications.
- Designating an entity at federal level (e.g., NTIA) to serve as advocate for the electromagnetic spectrum needs of local and state governments.
- Having FCC and NTIA follow up the PSWAC report recommendation through leading the development of a *National Public Safety Telecommunications Plan* and oversee its implementation.

We recommend state and local governments determine their readiness to deal with incidents, examine vulnerabilities and weaknesses in their systems that could be exploited to amplify the effects of incidents, and apply risk management techniques to deal with potential attacks.

(Intentionally Left Blank)

Appendix B

Glossary

Critical infrastructures span a vast and diverse set of industries, technologies, people, and traditions. This glossary provides a set of definitions and acronyms used to convey a common understanding of critical infrastructures in the context of this report.

Definitions

Attack: A discrete malicious action of debilitating intent inflicted by one entity upon another. A threat might attack a critical infrastructure to destroy or incapacitate it.

Banking and Finance: A critical infrastructure characterized by entities, such as retail and commercial organizations, investment institutions, exchange boards, trading houses, and reserve systems, and associated operational organizations, government operations, and support activities, that are involved in all manner of monetary transactions, including its storage for saving purposes, its investment for income purposes, its exchange for payment purposes, and its disbursement in the form of loans and other financial instruments.

Capability: The ability of a suitably organized, trained, and equipped entity to access, penetrate, or alter government or privately owned information or communications systems and/or to disrupt, deny, or destroy all or part of a critical infrastructure.

Combat: Activity of two or more entities taken in consideration of each other to achieve differing objectives. The military analogue of commercial competition.

Competition: Activity of two or more entities taken in consideration of each other to achieve differing objectives. The commercial analogue of military combat.

Critical Infrastructures: Infrastructures which are so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security.

Debilitated: A condition of defense or economic security characterized by ineffectualness.

Defense **(also *National Security*)**: The confidence that Americans' lives and personal safety, both at home and abroad, are protected and the United States' sovereignty, political freedom, and independence, with its values, institutions, and territory intact are maintained.

Destruction: A condition when the ability of a critical infrastructure to provide its customers an expected upon level of products and services is negated. Typically a permanent condition. An infrastructure is considered destroyed when its level of performance is zero.

Economic Security **(also *Global Economic Competitiveness*)**: The confidence that the nation's goods and services can successfully compete in global markets while maintaining or boosting real incomes of its citizens.

Electrical Power Systems: A critical infrastructure characterized by generation stations, transmission and distribution networks that create and supply electricity to end-users so that end-users achieve and maintain nominal functionality, including the transportation and storage of fuel essential to that system.

Emergency Services: A critical infrastructure characterized by medical, police, fire, and rescue systems and personnel that are called upon when an individual or community is responding to emergencies. These services are typically provided at the local level (county or metropolitan area). In addition, state and Federal response plans define emergency support functions to assist in response and recovery.

Gas and Oil Production, Storage and Transportation: A critical infrastructure characterized by the production and holding facilities for natural gas, crude and refined petroleum, and petroleum-derived fuels, the refining and processing facilities for these fuels and the pipelines, ships, trucks, and rail systems that transport these commodities from their source to systems that are dependent upon gas and oil in one of their useful forms.

Government Services: Sufficient capabilities at the Federal, state and local levels of government are required to meet the needs for essential services to the public.

Incapacitation**:** An abnormal condition when the level of products and services a critical infrastructure provides its customers is reduced. While typically a temporary condition, an infrastructure is considered incapacitated when the duration of reduced performance causes a debilitating impact.

Information and Communications: A critical infrastructure characterized by computing and telecommunications equipment, software, processes, and people that support:

- the processing, storage, and transmission of data and information,
- the processes and people that convert data into information and information into knowledge, and
- the data and information themselves.

Information or "Cyber" Security: Actions taken for the purpose of reducing system risk, specifically, reducing the probability that a threat will succeed in exploiting critical infrastructure vulnerabilities using electronic, RF, or computer-based means.

Infrastructure: The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of governments at all levels, and society as a whole.

Infrastructure Assurance: Preparatory and reactive risk management actions intended to increase confidence that a critical infrastructure's performance level will continue to meet customer expectations despite incurring threat inflicted damage. For instance, incident mitigation, incident response, and service restoration.

Infrastructure Protection: Proactive risk management actions intended to prevent a threat from attempting to or succeeding at destroying or incapacitating critical infrastructures. For instance, threat deterrence and vulnerability defense.

Intent: Demonstrating a deliberate series of actions with the objective of debilitating defense or economic security by destroying or incapacitating a critical infrastructure.

Natural Disaster: A physical capability with the ability to destroy or incapacitate critical infrastructures. Natural disasters differ from threats due to the absence of intent.

Partnership: A relationship between two or more entities wherein each accepts responsibility to contribute a specified, but not necessarily equal, level of effort to the achievement of a common goal. The public and private sector contributing their relative strengths to protect and assure the continued operation of critical infrastructures.

Physical Security: Actions taken for the purpose of restricting and limiting unauthorized access, specifically, reducing the probability that a threat will succeed in exploiting critical infrastructure vulnerabilities including protection against direct physical attacks, e.g., through use of conventional or unconventional weapons.

Public Confidence: Trust bestowed by citizens based on demonstrations and expectations of:

(1) Their government's ability to provide for their common defense and economic security and behave consistent with the interests of society; and

(2) Their critical infrastructures' ability to provide products and services at expected levels and to behave consistent with their customers' best interests.

Risk: The probability that a particular critical infrastructure's vulnerability will be exploited by a particular threat.

Risk Assessment: Produced from the combination of Threat and Vulnerability Assessments. Characterized by analyzing the probability of destruction or incapacitation resulting from a threat's exploitation of a critical infrastructure's vulnerabilities.

Risk Management: Deliberate process of understanding risk and deciding upon and implementing actions to reduce risk to an defined level. Characterized by identifying, measuring, and controlling risks to a level commensurate with an assigned value.

Sector: a) One of the two divisions of the economy (private or public); b) A group of industries or infrastructures which perform a similar function within a society. (e.g. vital human services)

Technology: Broadly defined, includes processes, systems, models and simulations, hardware, and software.

Threat: A foreign or domestic entity possessing both the capability to exploit a critical infrastructure's vulnerabilities and the malicious intent of debilitating defense or economic security. A threat may be an individual, an organization, or a nation.

Transportation: A critical infrastructure characterized by the physical distribution system critical to supporting the national security and economic well-being of this nation, including the national airspace system, airlines and aircraft, and airports; roads and highways, trucking and personal vehicles; ports and waterways and the vessels operating thereon; mass transit, both rail and bus; pipelines, including natural gas, petroleum, and other hazardous materials; freight and long haul passenger rail; and delivery services.

Vulnerability: A characteristic of a critical infrastructure's design, implementation, or operation of that renders it susceptible to destruction or incapacitation by a threat.

Vulnerability Assessment: Systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information, or product to determine the adequacy of

security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation.

Water Supply Systems: A critical infrastructure characterized by the sources of water, reservoirs and holding facilities, aqueducts and other transport systems, the filtration, cleaning and treatment systems, the pipelines, the cooling systems and other delivery mechanisms that provide for domestic and industrial applications, including systems for dealing with water runoff, waste water, and firefighting.

Acronyms

AAAE	—	American Association of Airport Executives
AAI	—	Alliance of American Insurers
AAPA	—	American Association of Port Authorities
AAR	—	Association of American Railroads
AASHTO	—	American Association of State Highway and Transportation Officials
ABA	—	American Bankers Association
ABIS	—	Advanced Battlefield Information System, DoD
ACEC	—	American Consulting Engineers Council
ACM-SIGOS	—	Association for Computing Machinery-Special Interest Group on Operating Systems
ACTD	—	Advanced Concepts Technology Demonstration
AFIWC	—	Air Force Information Warfare Center, DoD
AFTAC	—	Air Force Technical Applications Center, DoD
AGA	—	American Gas Association
AGCA	—	The Associated General Contractors of America
AIA	—	American Insurance Association
AICPA	—	American Institute of Certified Public Accountants
AID	—	Agency for International Development
AIIP	—	Association of Independent Information Professionals
ALPA	—	Air Line Pilots' Association
ANL	—	Argonne National Laboratory, DOE
ANSI	—	American National Standards Institute
ANSIR	—	Awareness of National Security Issues and Response, FBI

AOC — Association of Old Crows

APA — American Pilots Association

APCO — Association of Public-Safety Communications Officials-International, Inc.

API — American Petroleum Institute

APPA — American Public Power Association

APTA — American Public Transit Association

APWA — American Public Works Association

ARC — American Red Cross

ARPA — Advanced Research Projects Agency, DoD, predecessor to DARPA

ARPAnet — Advanced Research Projects Agency network, DoD, predecessor to the Internet

ASCC — Alaska Systems Coordinating Council

ASD — Assistant Secretary of Defense

ASIS — American Society for Industrial Security

ASLRA — The American Short Line Railroad Association

ASTM — American Society for Testing and Materials

ATA — Air Transportation Association of America; or
— American Trucking Associations, Inc.

ATC — Available Transmission Capacity

ATIS-NRSC — Alliance for Telecommunications Industry Solutions-Network Reliability Steering Committee

ATM — Asynchronous Transfer Mode

AWO — American Waterways Operators

AWWA — American Water Works Association

AWWARF — AWWA Research Foundation

B&F — Banking & Finance

BAFO — Best and Final Offer

BATF — Bureau of Alcohol, Tobacco and Firearms

BEA — Bureau of Export Administration, DOC

BECCA — Business Espionage Controls and Countermeasures Association

BIA — Bureau of Indian Affairs

BIOA — Bureau of International Organization Affairs, DOS

BLM — Bureau of Land Management

BLS	—	Bureau of Labor Statistics
BNL	—	Brookhaven National Laboratory, DOE
BOR	—	Bureau of Reclamation, DOI
BPA	—	Bonneville Power Administration
BRT	—	Bankers' Roundtable
CAAP	—	Critical Asset Assurance Program
CART	—	Computer Analysis and Response Team, FBI
CARVER	—	Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability
CATS	—	Consequences Assessment Tool Kit
CBDCOM	—	Chemical and Biological Defense Command, Army
CBO	—	Congressional Budget Office
CBOT	—	Chicago Board of Trade
CCIC	—	Committee on Computing, Information and Communications
CCIP	—	Center for Critical Infrastructure Protection
CCS	—	Common Channel Signaling network
CCTP	—	Common Criteria Testing Program, NIAP
CDC	—	Centers for Disease Control
CDRG	—	Catastrophic Disaster Response Group
CECOM	—	Communications Electronics Command, US Army
CEPACS	—	Centralized Emergency Preventive Automatic Control Systems: Electric reliability system used in Russia
CEQ	—	Council on Environmental Quality
CERT	—	Computer Emergency Response Team
CFAA	—	Computer Fraud and Abuse Act, 18 USC 1030
CFCA	—	Communications Fraud Control Association
CFIUS	—	Committee on Foreign Investment in United States
CFTC	—	Commodity Futures Trading Commission
CIA	—	Central Intelligence Agency
CIAC	—	Computer Incident Advisory Capability, DOE
CIDS	—	Computer Information Delivery Service
CINC	—	Commander in Chief
CIO	—	Chief Information Officer

CIP	—	Critical Infrastructure Protection
CIRG	—	Critical Incident Response Group, FBI
CISAC	—	Center for International Security and Arms Control, Institute for International Studies, Stanford University
CIST	—	Center for Information Security Technology, DOE
CITAC	—	Computer Investigations and Infrastructure Threat Assessment Center, FBI
CIWARS	—	Centre for Infrastructural Warfare Studies
CIWG	—	Critical Infrastructure Working Group, DOJ
CJCS	—	Chairman, Joint Chiefs of Staff
CJTF	—	Commander, Joint Task Force
CLIN	—	Community Learning Information Network, National Guard
CMC	—	Computer Malicious Code
CMDS	—	Computer Misuse and Detection System
CNA	—	Computer Network Attack
COAST	—	Computer Operations, Audit and Security Technology, Purdue University
COC	—	Council on Competitiveness
COE	—	Corps of Engineers
CONUS	—	Continental United States, the 48 contiguous States and the District of Columbia
COTS	—	Commercial Off-The-Shelf products
CPAS	—	Cellular Priority Access Services
CPSC	—	Consumer Product Safety Commission
CSA	—	Computer Security Act of 1987
CSAAS	—	Combat Support Agency Assessment System
CSG	—	Coordinating Sub-Group
CSG/CT	—	Coordinating Sub-Group/Counterrorism
CSI	—	Computer Security Institute
CSPP	—	Computer Systems Policy Project
CSRC	—	Computing Sciences Research Center; — Computer Security Resource Clearinghouse; — Collaborative Software Resource Center; or — Computer Safety and Reliability Center
CSRL	—	Computer Security Research Laboratory, University of California at Davis
CSSPAB	—	Computer System Security and Privacy Advisory Board, NIST

CSTB	—	Computer Science and Telecommunications Board, National Research Council
CUEA	—	California Utilities Emergency Association
CVA	—	Computer Virus Association
DARPA	—	Defense Advanced Research Projects Agency, DoD
DASD	—	Deputy Assistant Secretary of Defense
DCI	—	Director of Central Intelligence
DCS	—	Defense Communications System
DDNSCC	—	Defense Data Network Security Coordination Center, DoD
DEA	—	Drug Enforcement Administration
DECA	—	Development of Espionage, Counterintelligence, and Counterterrorism Awareness, FBI
DEST	—	Domestic Emergency Support Team, FBI
DHHS	—	Department of Health and Human Services, United States
DIA	—	Defense Intelligence Agency, DoD
DII	—	Defense Information Infrastructure
DIN	—	Defense Intelligence Network, DoD
DIS	—	Defense Investigative Service; or
	—	Disruption Impact Simulator Model
DISA	—	Defense Information Systems Agency, DoD
DLA	—	Defense Logistics Agency
DNS	—	Domain Name System for Internet
DOC	—	Department of Commerce, United States
DoD	—	Department of Defense, United States
DoDD	—	Department of Defense Directive
DOE	—	Department of Energy, United States
DOEd	—	Department of Education, United States
DOJ	—	Department of Justice, United States
DOI	—	Department of Interior, United States
DOL	—	Department of Labor, United States
DOMS	—	Director of Military Support, DoD
DOS	—	Department of State, United States
DOT	—	Department of Transportation, United States

DOTr — Department of the Treasury, United States

DPA — Defense Production Act of 1950 (50 USC App 2061 et seq.)

DRA — Defense Relief Act, Title V, Stafford Act

DS — Bureau of Diplomatic Security, DOS

DSB — Defense Science Board

DSWA — Defense Special Weapons Agency

DTC — Depository Trust Company

EAM — Existing Assurance Measures

EAS — Emergency Alert System, FCC

ECAR — East Central Area Reliability Coordination

ECPA — Electronic Communications Privacy Act of 1986

ED — Department of Education, United States

EEA — Economic Espionage Act of 1996

EEI — Edison Electric Institute; or
— Essential Elements of Information

EEOC — Equal Employment Opportunity Commission

EFLEA — Emergency Federal Law Enforcement Assistance, DOJ

EIA — Energy Information Administration, DOE

ELCON — Electricity Consumers Resource Council

EMP — Electromagnetic Pulse

EMS — Emergency Medical Services

EO — Executive Order

EOP — Executive Office of the President

EPA — Environmental Protection Agency

EPIC — Electronic Privacy Information Center

EPPA — Employee Polygraph Protection Act

EPRI — Electric Power Research Institute

EPSA — Electric Power Supply Association

ERA — Economic Regulatory Administration, DOE

ERNS — Emergency Response Notification System, EPA

ERAP — Emergency Response Assistance Program, DoD

ERCOT — Electric Reliability Council of Texas

ERRI — Emergency Response and Research Institute

ESRTF — Electric System Reliability Task Force, DOE

ETEC — Energy Technology Engineering Center, DOE

EU-BDC — Explosives Unit-Bomb Data Center, FBI

EW — Electronic Warfare

FAA — Federal Aviation Administration, DOT

FACA — Federal Advisory Committee Act

FACSPMF — Federal Agency Computer Security Program Managers' Forum, NIST

FASB — Financial Accounting Standards Board

FBI — Federal Bureau of Investigation

FCC — Federal Communications Commission

FCRA — Federal Fair Credit Reporting Act

FDA — Food and Drug Administration

FDIC — Federal Deposit Insurance Corporation

FEDCIRC — Federal Computer Incident Response Capability

FEDNET — Federal Reserve System Network, FRS

FEMA — Federal Emergency Management Agency

FEPPA — Federal Employee Polygraph Protection Act

FERC — Federal Energy Regulatory Commission

FEST — Foreign Emergency Support Team, DOS

FFB — Federal Financing Bank

FFIEC — Federal Financial Institutions Examination Council

FFRDC — Federally Funded Research and Development Center

FHWA — Federal Highway Administration, DOT

FICA — Federal Insurance Contributions Act

FinCEN — Financial Crimes Enforcement Network, Treasury

FIRMR — Federal Information Resource Management Regulation

FIRST — Forum of Incident Response and Security Teams, NIST

FISSEA — Federal Information Systems Security Association

FMC — Federal Maritime Commission

FOIA — Freedom of Information Act

FOSC — Federal On-Scene Coordinators, USCG

FRA — Federal Railroad Administration, DOT
FRCC — Florida Reliability Coordinating Council
FRB — Federal Reserve Board
FRP — Federal Response Plan, FEMA
FRS — Federal Reserve System
FSLIC — Federal Savings and Loan Insurance Corporation
FSTC — Financial Services Technology Consortium
FSTS — Federal Secure Telephone Service
FTA — Federal Transit Administration, DOT
FTC — Federal Trade Commission
FTS — Federal Telecommunications System
GAAP — Generally Accepted Accounting Principles
GAAS — Generally Accepted Auditing Standards
GAGAS — Generally Accepted Government Auditing Standards
GAO — Government Accounting Office
GASB — Government Accounting Standards Board
GASSP — Generally Accepted System Security Principles
GCCS — Global Command and Control System
GETS — Government Emergency Telecommunications Service, NCS
GII — Global Information Infrastructure
GIS — Geographic Information Systems
GISB — Gas Industry Standards Board
GITSB — Government Information Technology Services Board, OMB
GNP — Gross National Product
GOTS — Government Off-The-Shelf products
GPRA — Government Performance and Results Act
GPS — Global Positioning System
GRI — Gas Research Institute
GSA — General Services Administration
HUMINT — Human Intelligence
I&C — Information and Communications
IA — Information Assurance

IACP — International Association of Chiefs of Police

IAFC — International Association of Fire Chiefs

IASO — Information Assurance Support Office, recommended by PCCIP

IATF — Information Assurance Task Force, NSTAC

IAWC — Information Analysis and Warning Center, recommended by PCCIP

IBWC — International Boundary and Water Commission, US Department of State

IC — Intelligence Community

ICI — Investment Company Institute

ICBM — Intercontinental Ballistic Missile

IDA — Institute for Defense Analyses

IDS — Intrusion Detection System

IEEE — Institute of Electrical and Electronic Engineers

IETF — Internet Engineering Task Force

IG — Inspector General

IGT — Institute of Gas Technology

IIA — The Institute of Internal Auditors

IIPLR — Insurance Institute for Property Loss Reduction

IITF — Information Infrastructure Task Force

IMINT — Imagery Intelligence

IMPWG — Information Management Policy Working Group

INEL — Idaho National Engineering Laboratory, DOE

INFOSEC — Information Security

INGAA — Interstate Natural Gas Association of America

INR — Bureau of Intelligence and Research, DOS

INSS — Institute for National Strategic Studies, National Defense University

InterNIC — Internet Network Information Center

IO — Information Operations

IOTC — Information Operations Technology Center, DoD-CIA

IPAA — Independent Petroleum Association of America

IPCG — Infrastructure Protection Coordinating Group

IPTF — Infrastructure Protection Task Force

IRD — Incident Response Division, NRC

ISAC — Industrial Security Advisory Council

ISACA — Information Systems Audit and Control Association

ISO — International Standards Organization

ISOO — Information Security Oversight Office, GSA

ISP — Internet Service Provider

ISPAC — Information Security Policy Advisory Council

ISSA — Information Systems Security Association

ISSB — Information Systems Security Board, NSTAC

ISSO — Information Security Oversight Office, OMB

ISSP — Information Systems Security Program, DoD

ISSR — Information System Security Research-Joint Technology Office, DoD

ISTA — Intelligence, Surveillance and Target Acquisition

IT — Information Technology

ITAA — Information Technology Association of America

ITC — International Trade Administration, Department of Commerce

ITI — Information Technology Industry Council

ITL — Information Technology Laboratory, NIST

ITMRA — Information Technology Management Reform Act of 1996

ITS — Intelligent Transportation System, DOT

I&W — Indications and Warning

I&W/TA — Indication and Warning/Threat Assessment

IW — Information Warfare

IW-D — Information Warfare-Defense

JCEWS — Joint Command, Control and Electronic Warfare School

JICPAC — Joint Intelligence Command, Pacific

JIGSAG — Joint Industry Government Security Awareness Group

JIWAR — Journal of Infrastructural Warfare

JPO-STC — Joint Project Office for Special Technology Countermeasures, DoD

JRC — Joint Review Council, FAA

JWAC — Joint Warfare Analysis Center

KMI — Key Management Infrastructure

LAN — Local Area Network; or Local Access Network

LANL — Los Alamos National Laboratory, DOE
LBL — Lawrence Berkeley National Laboratory, DOE
LDC — Local Distribution Company
LLNL — Lawrence Livermore National Laboratory, DOE
LNG — Liquefied Natural Gas
LOOP — Louisiana Offshore Oil Platform
LPG — Liquefied Petroleum Gas
LSNWG — Large Scale Networking Working Group
MAAC — Mid-Atlantic Area Council
MAIN — Mid-America Interconnected Network
MAPP — Mid-Continent Area Power Pool
MARAD — Maritime Administration
MASINT — Measurement and Signature Intelligence
MEII — Minimum Essential Information Infrastructure
MILNET — Military Network, unclassified packet-switched network
MISSI — Multilevel Information Systems Security Initiative, NSA
MOU — Memorandum of Understanding, EPA
NACHA — National Automated Clearing House Association
NACIC — National Counterintelligence Center
NACo — National Association of Counties
NAFTA — North American Free Trade Agreement
NANOG — North American Network Operators Group
NARUC — National Association of Regulatory Utility Commissioners
NAS — National Academy of Sciences; or National Airspace System
NASDV — National Association of Security and Data Vaults
NASIO — National Association of State Information Officers
NASIRE — National Association of State Information Resource Executives
NATO — North American Treaty Organization
NAWC — National Association of Water Companies
NCC — National Counterintelligence Center
NCCCD — National Center for Computer Crime Data
NCCS — National Computer Crime Squad, FBI

NCIC — National Criminal Information Center, FBI

NCMS — National Classification Management Society

NCS — National Communications System, consortium of 23 Federal agencies

NCSA — National Computer Security Association

NCSC — National Computer Security Center, NSA

NCSL — National Conference of State Legislatures

NDP — National Defense Panel

NDU — National Defense University

NEC — National Economic Council

NEMA — National Emergency Management Agency or Association

NENA — National Emergency Number Association

NERC — North American Electric Reliability Council

NFPA — National Fire Protection Association

NGA — National Governors' Association

NGAUS — National Guard Association of the United States

NGI — Next Generation Internet

NGWA — National Ground Water Association

NIAP — National Information Assurance Partnership, NIST-NSA

NIAC — National Infrastructure Assurance Council, recommended by PCCIP

NIC — National Intelligence Council

NIGP — National Institute of Governmental Purchasing

NII — National Information Infrastructure

NIITF — National Information Infrastructure Task Force, NSTAC

NIST — National Institute of Standards and Technology, DOC

NITL — National Industrial Transportation League

NLC — National League of Cities

NMCC — National Military Command Center

NMSS — Nuclear Material Safety and Safeguards, NRC

NN — Non-Proliferation and National Security, DOE

NOAA — National Oceanic and Atmospheric Administration

NORAD — North American Air Defense Command

NPC — National Petroleum Council, DOE

NPCC — Northeast Power Coordinating Council

NPHI — National Pipeline Hazard Index

NPR — National Performance Review

NPRA — National Petroleum Refiners Association

NPSTC — National Public Safety Telecommunications Council

NRC — Nuclear Regulatory Commission;
— National Research Council; or
— National Response Center (USCG)

NRECA — National Rural Electric Cooperative Association

NREL — National Renewable Energy Laboratory, DOE

NRIC — Network Reliability and Interoperability Council, FCC

NRL — Naval Research Laboratory, DoD

NRRI — National Regulatory Research Institute, NARUC

NRT — National Response Team

NRWA — National Rural Water Association

NSA — National Security Agency

NSC — National Security Council

NSCC — National Securities Clearing Corporation

NSDD — National Security Decision Directive

NS/EP — National Security and Emergency Preparedness

NSF — National Science Foundation

NSI — Network Solutions Inc., operates Internet domain name system

NSIE — Network Security Information Exchange, NSTAC

NSS — National Security Strategy

NSTAC — National Security Telecommunications Advisory Committee, President

NSTC — National Science and Technology Council

NSTISSC — National Security Telecommunications and Information Systems Security Committee

NTCA — National Telephone Cooperative Association

NTIA — National Telecommunications and Information Administration, DOC; or
— National Telecommunications Industry Association

NTIS — National Technical Information Service

NTSB — National Transportation Safety Board

NUG — Non-Utility Generator

NVLAP — National Voluntary Laboratory Accreditation Program, NIST

NYSE — New York Stock Exchange

OASIS — Open Access Same-time Information System

OCC — Office of the Comptroller of the Currency, Treasury

OCIIP — Office of Computer Investigations and Infrastructure Protection, FBI

OCONUS — All domestic and foreign territories Outside of CONUS

OECD — Organization of Economic Cooperation and Development

OET — Office of Emergency Transportation, DOT

OHMS — Office of Hazardous Materials Safety, DOT

OIRA — Office of Information and Regulatory Affairs, OMB

OMB — Office of Management and Budget

ONI — Office of Naval Intelligence

ONIA — Office of National Infrastructure Assurance, recommended by PCCIP

OPEC — Organization of Petroleum Exporting Countries

OPM — Office of Personnel Management

OPS — Office of Pipeline Safety, DOT

ORNL — Oak Ridge National Laboratory, DOE

OSAC — Overseas Security Advisory Council, DOS

OSHA — Occupational Safety and Health Administration

OST — Office of the Secretary of Transportation

OSTP — Office of Science and Technology Policy

OTS — Office of Thrift Supervision

PACOM — US Pacific Command

PBX — Private Branch Exchange

PCCIP — President's Commission on Critical Infrastructure Protection

PD — Physical Distribution

PEAD — Presidential Emergency Action Document

PGM — Precision Guided Munitions

PHS — Public Health Service, DHHS

PMA — Power Marketers Association

PNWL — Pacific Northwest National Laboratory, DOE

PSN	—	Public Switched Network
PSTN	—	Public Switched Telephone Network
PSWAC	—	Public Service Wireless Advisory Committee, FCC, NTIA, disbanded, succeeded by NPSTC
PTN	—	Public Telecommunications Network
PWGFM	—	President's Working Group on Financial Markets
QDR	—	Quadrennial Defense Review
RAA	—	Regional Airline Association
RAC	—	Rebuild America Coalition
RCCC	—	Regular Common Carrier Conference
R&D	—	Research and Development
RF	—	Radio Frequency
RIN	—	Real-time Information Network
RRIS	—	Rapid Response Information System, FEMA
RSPA	—	Research and Special Programs Administration, DOT
RUS	—	Rural Utilities Service, US Department of Agriculture
RVWG	—	Reliability and Vulnerability Working Group, IITF
SAFE	—	Security and Freedom through Encryption Act, pending before Congress
SBA	—	Small Business Administration
SCADA	—	Supervisory Control And Data Acquisition system
SCC	—	Security Coordinator Subcommittee, NERC
SCIP	—	Society of Competitive Intelligence Professionals
S/CT	—	Office of the Coordinator for Counterterrorism, DOS
SEC	—	Securities and Exchange Commission
SECDEF	—	Secretary of Defense
SEI	—	Software Engineering Institute, Carnegie Mellon University
SERC	—	Southeastern Electric Reliability Council
SIA	—	Security Industry Association
SIAC	—	Securities Industry Automation Corporation
SIF	—	Security Issues Forum, IITF
SIGINT	—	Signals Intelligence
SIOP	—	Single Integrated Operations Plan

SIOPNET	—	Single Integrated Operational Plan Network
SIPRNET	—	Secret Internet Protocol Routing Network
SLBM	—	Submarine Launched Ballistic Missile
SNAC	—	Systems and Networks Attack Center, NSA
SNL	—	Sandia National Laboratories, DOE
SOCOM	—	Special Operations Command, DoD
SONET	—	Synchronous Optical Network
SORTS	—	Status of Resources and Training System
SPA	—	Software Publishers Association
SPB	—	Security Policy Board
SPP	—	Southwest Power Pool
SPR	—	Strategic Petroleum Reserve
SPSSTF	—	Security Process Support System Task Force, NERC
STORET	—	Storage and Retrieval Water Quality Data Base, EPA
SVRR	—	Sluzhba Vneshney Rasvedi Rossi, the successor to the KGB, the Russian intelligence service
SWIFT	—	Society for Worldwide Interbank Financial Telecommunication
TAPS	—	Trans-Alaska Pipeline System
TCP	—	Technology Control Plan
TIA	—	Telecommunications Industry Association
TIS	—	Terrorist Information System, FBI
TOR	—	Terms of Reference
TSI	—	Transportation Safety Institute, DOT
TSP	—	Telecommunications Service Priority, NCS
TSWG	—	Technical Support Working Group, DoD
TTAP	—	Trusted Technology Assessment Program, NIST
TVA	—	Tennessee Valley Authority
USAF	—	United States Air Force
USC	—	United States Code
USCG	—	United States Coast Guard
USCM	—	United States Conference of Mayors
USDA	—	United States Department of Agriculture

USEA — United States Energy Association
USGS — United States Geological Survey
USIA — United States Information Agency
USMC — United States Marine Corps
USN — United States Navy
USRA — United States Railway Association
USSC — United States Sentencing Commission
USTA — United States Telephone Association
UTC — Utility Telecommunications Council
VTS — Vessel Traffic Service
WAAS — Wide Area Augmentation System
WAPA — Western Area Power Administration
WARM — War-time Mode
WMD — Weapons of Mass Destruction or Disruption
WQA — Water Quality Association
WRC — Water Resources Council
WSCC — Western Systems Coordinating Council
WSTB — Water Science and Technology Board, National Research Council
XIWT — Cross-Industry Working Team